PROCEEDINGS OF THE INTERNATIONAL
CRISIS AND RISK COMMUNICATION CONFERENCE
MARCH 9-11, 2020. ORLANDO FL, USA

Mind the gap: Understanding stakeholder reactions to different types of data security

Audra Diers-Lawson

Leeds Beckett University
Leeds, United Kingdom

Amelia Symons

Leeds Beckett University
Leeds, United Kingdom

Abstract: Data security breaches are an increasingly common problem for organizations, yet there are critical gaps in our understanding of how different stakeholders understand and evaluate organizations that have experienced these kinds of security breaches. While organizations have developed relatively standard approaches to responding to security breaches that: (1) acknowledge the situation; (2) highlight how much they value their stakeholders' privacy and private information; and (3) focus on correcting and preventing the problem in the future, the effectiveness of this response strategy and factors influencing it have not been adequately explored. This experiment focuses on a 2 (type of organization) x 2 (prior knowledge of breach risk) with a control group design. Findings suggest that perceptions of competence is the most important factor influencing outcome variables like behavioral intention and social responsibility evaluations.

Keywords — competence, crisis communication, data security breach, stakeholder relationship management

---

SUGGESTED CITATION: Diers-Lawson, A,. & Symons, A. (2020). Mind the gap: Understanding stakeholder reactions to different types of data security. *Proceedings of the International Crisis and Risk Communication Conference*, *Volume 3* (pp. 25-28). Orlando Fl: Nicholson School of Communication and Media. https://www.doi.org/10.30658/icrcc.2020.6

INTRODUCTION

Both industry and academic publications define data breaches as incidents where private or confidential information – especially medical and/or financial records – are put at risk of exposure [1]. In IBM's *Cost of a Data Breach Report* [1], three primary causes are identified – criminal attacks, system glitches (i.e., technical errors), and human error. The report found that the average cost of lost business for organizations in 2019 was $1.42 million (USD) and affected customer turnover by 3.9 percent. In fact, two-thirds of people report being less likely to do business with an organization that has experienced a breach where financial and/or sensitive information was stolen [2]. This paper explores the factors influencing data breaches and tests them in an experiment. We will briefly highlight the background on data breaches, introduce the experiment, and report on the results.

LITERAURE REVIEW

Data breaches are not merely a technical problem for organizations to solve. IBM [1] points out that the cost of the breach will vary based on the cause as well as the risk mitigation processes put in place ahead of the breach. The report found that much of the cost of the data breach was in the reputational and trust damage done to organizations affected by the breaches. The IBM report also found that organizations with effective incident response teams and extensive testing of their response teams saved millions. Likewise, academic research from the field of information systems management points out that damage control is as much a function of reputation management and good communication with stakeholders as it is technically managing the breach [3, 4, 5].

ISSN: 2576-9111

https://doi.org/10.30658/icrcr.2020.6

There is, however, a dearth of public relations research directly exploring data breaches despite their growing impact and direct communicative implications. Existing research identifies the limitations and need for empirical studies of the role of public relations before, during, and after data breaches [3, 5]. Even where public relations research has explored data breaches, it often focuses on the connections between reputation in a social media context [6] or with analyses of organizational responses and other indirect measures of stakeholder attitudes instead of direct measures [4, 5]. Yet findings from the few studies directly connecting data breaches and stakeholder attitudes, suggest that investing in stakeholder relationship development and management with holds critical value for organizations who may experience these types of crises [7].

Moreover, there are indications that many of crisis communication's assumptions about the effectiveness of the 'right' kind of crisis response may not be realized in the data. For example, counter to previous findings, Bakker, van Bommel, Kerstolt, and Giebels [8] found that specific crisis response messages had little to no direct effect on outcome measures. There are also divergent findings in the literature about specific strategies applied across situations [9], so it is difficult to generate reliable and actionable communication recommendations for post crisis response. At the same time, there are clear findings that pre-crisis relationships between organizations, stakeholders, and issues have been found to meaningfully affect stakeholder attitudes about organizations in crisis and coupled with research demonstrating the impact stakeholder emotion invoked by the crisis itself, the question we should be broadly asking is what factors matter in predicting stakeholder response to data breaches?

METHODS

In brief, this experiment was a a 2 (type of organization) x 2 (prior knowledge of breach risk) with a control group design with random assignment into groups. British participants (N = 221) were introduced to a scenario where their private details were compromised by hackers. The information accessed illegally was either in their bank or with their doctor's office (type of organization). These institutions were selected because of the frequency with which information from them is leaked and because financial and health data is often regarded as the most private. Second, the situation was put in context where either the organization had been warned about the possibility of the hack ahead of time and failed to act or was hacked despite having the latest safeguards and no advance warning (prior knowledge of breach risk). The manipulation checks demonstrate respondents correctly understood the information presented to them with a one-way ANOVA and Scheffe post hoc confirming significant differences in the correct identification of each condition (F (4, 323) = 57.54, p < .00).

Using the stakeholder relationship model [10] as a guide, the experimental condition, blame attribution, competence, stakeholder attributes and attitudes, statement effectiveness, trustworthiness, and reputation were all correlated with outcome variables for support for the organization, social responsibility evaluation, and behavioral intention to keep using the affected organization. Significantly correlated factors were then entered into a multiple hierarchical regression in order to evaluate causal factors influencing the outcomes.

RESULTS

Overall, while these data confirm that the type of organization (i.e., banks or doctor's offices) and level of material blame influence the relationships between organizations and issues (i.e., blame and data security competence), organizations and stakeholders (i.e., social responsibility, trustworthiness, and reputation), response effectiveness, as well as outcomes (behavioral intention, organizational support, and reputational damage), they only account for about eight to nine percent of the total variation. This suggests exploring the other factors is critical if we are to understand how the relational and communication dynamics influence an organization's data breach crisis experience.

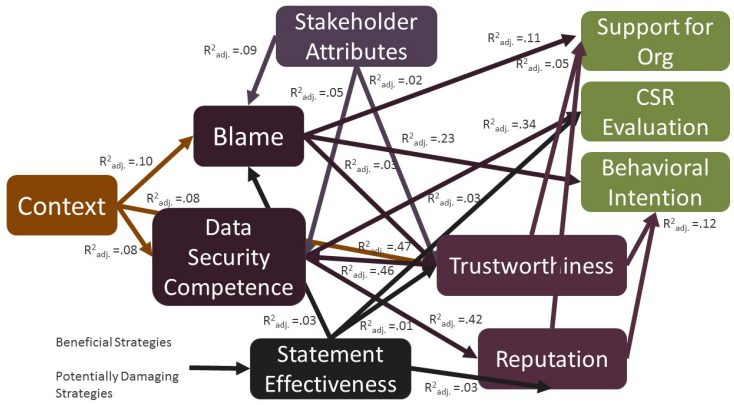

Figure 1: Summary of Results 1

Figure 1 summarizes the critical findings for this research. First, we explored the relationship between the organization and the issue of data breaches by analyzing the factors driving stakeholder attitudes about blame and competence, these data demonstrate that context (i.e., industry * material blame) are important as noted but are not the most critical factor in predicting stakeholder attitudes. Instead an organization's trustworthiness is the most significant predictor of an organization's competence during a data breach.

Blame assignment is a complex construct where stakeholders mix together their understanding of the situation, type of organization, their own attitudes and experiences with an evaluation of the organization's response to the situation. However, there is yet a lot that is unknown about blame attribution in data breaches because despite the variables tested, the overall adjusted r-squared was still only .22. This suggests that even though it is typically used in crisis communication as a critical predictor, the field still has a limited understanding of it in crises from a predictive perspective.

Second, we analyzed those factors driving stakeholder attitudes about the organization and focused on whether the organization is viewed as socially responsible, trustworthy, and has a good reputation because previous research suggests these are the most critical evaluations that stakeholders make (see Figure 1). These findings suggest that while situation (i.e., industry and material blame) provide some insight into explaining some emergent attitudes, the two critical factors that explain stakeholder evaluations of organizations facing data breaches are the organization's competence and appropriateness of the crisis response statement.

These data also found that both material blame and blame attribution were insignificant once stakeholders' judgements about the organization's data security competence were taken into account. This suggests that people generally acknowledge that data security risks exist in a modern environment, but what people want to know is that not only does the organization do everything they can to mitigate those risks but when a breach happens the organization responds well. If we think of social responsibility, trustworthiness, and reputation as judgements, then the organization's relationship to the issue – especially its demonstrated competence is a proxy for these valuations. Therefore, if an organization proves its competence on an issue, we would expect that evaluations of it as a socially responsible and trustworthy organization would meaningfully improve as would its reputation. In short – organizations must show their effectiveness in responding to crises, not just tell their stakeholders about it.

In this context, if people need to see the organization acting, how should organizations communicate about it? This was divided into two related questions – evaluating the components that improve crisis response messaging during security breaches and identifying if the context (industry * material blame) affected the message's effectiveness. For the most part, these data demonstrate that context did not influence how effective messages were viewed. This suggests that during most kinds of data breaches what a desirable message looks like is consistent. These data suggest that stakeholders are willing to listen to what the organization has to say and expects to hear information rich accounts of how the organization is going to safeguard and protect the stakeholders both now and in the future. However, these data also found that strategies focused on self-promotion, defensiveness, and talking about the organization are undesirable and could damage stakeholders' impressions of the organization. In short, organizations should not be talking about themselves, they should be talking about the issue and the stakeholders' interests.

Finally, taking all of these factors into account, Figure 1 demonstrates that we can account for approximately 40% of stakeholder behavioral intention and 22% of more general support for the organization experiencing a data breach based on a combination of understanding the context (industry * material blame), the organization's relationship to the issue (i.e., blame and competence), and the stakeholders' relationship to the organization (trustworthiness, social responsibility, and reputation). While stakeholder attitudes and messaging are important, these data suggest they are mediating variables rather than direct predictors of the outcomes. These data suggest very clearly then that the role of public relations and crisis management begins long before a crisis occurs, and responses must reflect both the substance of both concrete actions the organization has taken or takes along with the quality of the relationship that it has built with its stakeholders in order to be successful.

CONCLUSION

When the findings from this study are taken together, there are four conclusions that we can draw. First, broadly the field of communication often assumes that the purpose of communicating with stakeholders is about changing or reaffirming behavioral intention. However, in this case it does not directly influence behavioral intention; instead communication effectiveness functions as a mediating variable that affects how stakeholders judge the organization and not the outcomes directly. Communication therefore can influence blame attribution, trustworthiness, and reputation all of which affects the behavioral intention. This is one of the reasons why messages should be information rich and focused on the organization's actions and not the organization itself.

Second, the need to communicate about the organization's findings is explained by predictive value of understanding stakeholder evaluations of the organization's competence. If an organization can demonstrate competence in managing the issue – in this case data security breaches – then we would expect that evaluations of it as a socially responsible and trustworthy organization would meaningfully improve as would its reputation – showing and not telling stakeholders that the organization is 'good'.

Third, these data are specific to data security breaches and within a British context. The question as to whether these findings would remain predictive in other cultural and crisis contexts certainly needs testing. However, at present, these findings provide an important piece of intelligence about how organizations should be responding to the increasingly common problem of data security breaches.

Finally, these data suggest that while situational or contextual factors like industry and the type of crisis remain important, they are not driving the stakeholder evaluations of organizations facing data security breaches. It calls into question the field's focus on crisis type and industry as being instrumental in how practitioners design crisis response messages. Of course, these findings need to be tested across multiple contexts, but provide a strong grounding for focusing on the relational and not situational factors influencing crises.

Author Biography

Audra Diers-Lawson (Ph.D. University of Texas at Austin) is a Senior Lecturer at Leeds Beckett University, UK. audra.lawson@leedsbeckett.ac.uk

Amelia Symons (B.A. Leeds Beckett University)

REFERENCES

[1] *2019 Cost of a Data Breach Report*. (2019). Retrieved from https://www.ibm.com/security/data-breach.

[2] Graham, A. (2019). Infographic: List of data breaches in 2018.

[3] Choi, B. C., Kim, S. S., & Jiang, Z. (2016). Influence of firm's recovery endeavors upon privacy breach on online customer behavior. *Journal of management information systems, 33*(3), 904-933.

[4] Gwebu, K. L., Wang, J., & Wang, L. (2018). The role of corporate reputation and crisis response strategies in data breach management. *Journal of management information systems, 35*, 683-714. https://doi.org/10.1080/07421222.2018.1451962

[5] Wang, P., & Park, S.-A. (2017). Communication in cybersecurity: A public communication model for business data breach incident handling. *Issues in Information Systems, 18*(2), 136-147.

[6] Confente, I., Siciliano, G. G., Gaudenzi, B., & Eickhoff, M. (2019). Effects of data breaches from user-generated content: A corporate reputation analysis. *European Management Journal, 37*, 492-504. https://doi.org/10.1016/j.emj.2019.01.007

[7] Jahng, M. R., & Hong, S. (2017). How should you tweet?: The effect of crisis response voices, strategy, and prior brand attitude in social media crisis communication. *Corporate reputation review, 20*, 147-157. https://doi.org/10.1057/s41299-017-0022-7

[8] Bakker, M. H., van Bommel, M., Kerstholt, J. H., & Giebels, E. (2018). The influence of accountability for the crisis and type of crisis communication on people's behavior, feelings and relationship with the government. *Public Relations Review, 44*, 277-286. https://doi.org/10.1016/j.pubrev.2018.02.004

[9] Fuoli, M., van de Weijer, J., & Paradis, C. (2017). Denial outperforms apology in repairing organizational trust despite strong evidence of guilt. *Public Relations Review, 43*, 645-660. https://doi.org/10.1016/j.pubrev.2017.07.007

[10] Diers-Lawson, A. (2020). *Crisis Communication: Managing Stakeholder Relationships*. London: Routledge.