Building Crisis Capacity with Data Breaches: The Role of Stakeholder Relationship Management and Strategic Communication

Audra Diers-Lawson
Senior Lecturer
Leeds Beckett University, Leeds UK
audra.lawson@leedsbeckett.ac.uk

Amelia Symons
Leeds Beckett University, Leeds UK

Cheng Zeng
Assistant Professor
North Dakota State University, Fargo, ND USA

Abstract
Purpose – Data security breaches are an increasingly common and costly problem for organizations, yet there are critical gaps in our understanding of the role of stakeholder relationship management and crisis communication in relation to data breaches. In fact, though there have been some studies focusing on data breaches, little is known about what might constitute a "typical" response to data breaches whether those responses are effective at maintaining the stakeholders' relationship with the organization, their commitment to use the organization after the crisis, or the reputational threat of the crisis. Further, even less is known about the factors most influencing response and outcome evaluation during data breaches.

Design/methodology/approach – We identify a "typical" response strategy to data breaches and then evaluate the role of this response in comparison to situation, stakeholder demographics and relationships between stakeholders, the issue and the organization using an experimental design. This experiment focuses on a 2 (type of organization) 3 2 (prior knowledge of breach risk) with a control group design.

Findings – Findings suggest that rather than employing reactive crisis response messaging the role of public relations should focus on proactive relationship building between organizations and key stakeholders.

Originality/value – For the last several decades much of the field of crisis communication has assumed that in the context of a crisis the response strategy itself would materially help the organization. These data suggest that the field crisis communication may have been making the wrong assumption. In fact, these data suggest that reactive crisis response has little-to-no effect once we consider the relationships between organizations, the issue and stakeholders. The findings show that an ongoing program of crisis capacity building is to an organization's strategic advantage when data security breaches occur.

Keywords UK, Strategic communication, Crisis response, Data breach, Crisis capacity, Stakeholder relationship model

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 (*2019 Cost of a Data Breach Report*, 2019; Kim, Johnson, & Park, 2017). In IBM's *Cost of a Data Breach Report* (2019), three primary causes are identified – criminal attacks, system glitches (i.e., technical errors), and human error. The report found 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 (Graham, 2019).

Unfortunately, the problem of data breaches is also increasing each year (Gwebu, Wang, & Wang, 2018). Figure 1 summarizes the annual data on global security breaches, that have been reported by the media and suggest that while system glitches vary year-by-year, the growth and reporting of criminal attacks on organizations has grown by 270 percent in just two years leading to an annual global loss of more than 2.8 billion data records in 2019 (Graham, 2018, 2019; Irwin, 2020). In practical terms, it is much more likely that both organizations and their stakeholders have already been directly affected by a data breach and the nearly exponential growth trends represents a critical risk. The 2020 COVID-19 global pandemic further highlighted data protection vulnerabilities as organizations globally scrambled to manage the transition from traditional work routines to virtual work environments. For example, a reported 71 percent of British business decision-makers believing the shift to remote working has increased their risk of data breach (Sullivan, 2020).

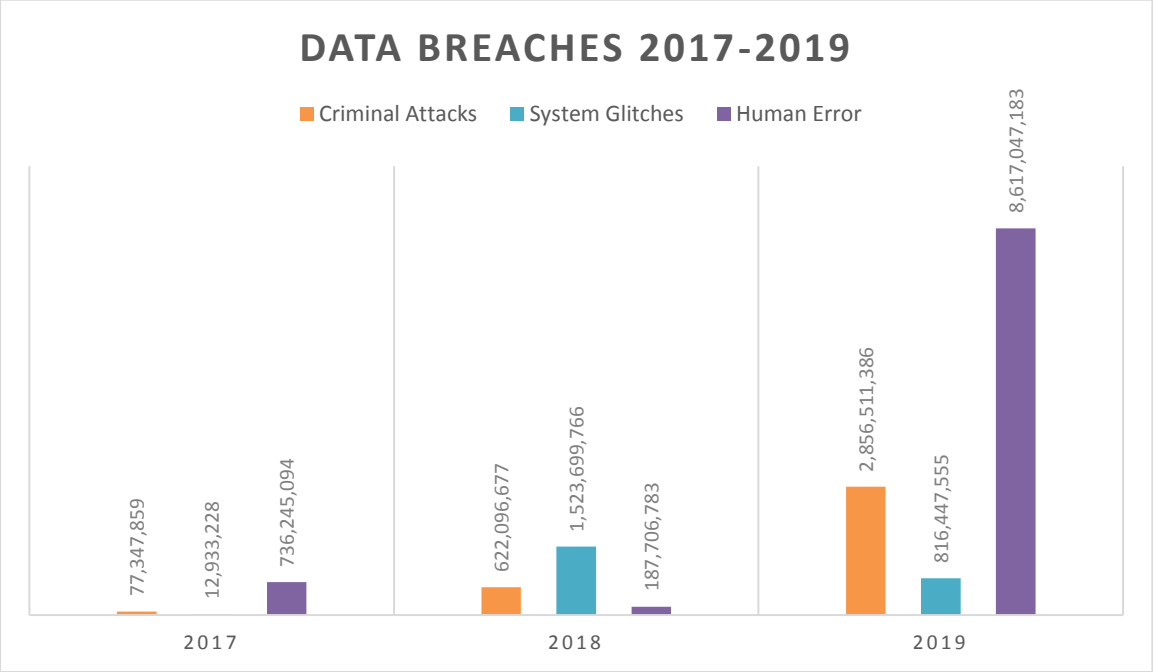

Figure 1. Summary of the global data breaches from 2017-2019 based on IT Governance's Annual Reports

Data breaches are not merely a technical problem for organizations to solve. IBM (2019) 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 (Angst, Block, D'arcy, & Kelley, 2017; Choi, Kim, & Jiang, 2016; Gwebu et al., 2018; Syed, 2019; Wang & Park, 2017).

There is, however, a dearth of 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 strategic communication before, during, and after data breaches (Choi et al., 2016; Rosati, Deeney, Cummins, Van der Werff, & Lynn, 2019; Wang & Park, 2017). Even where crisis research has explored data breaches, it often focuses on the connections between reputation in a social media context, such as how users might tweet about cyber-attacks (Confente, Siciliano, Gaudenzi, & Eickhoff, 2019; Vogler & Meissner, 2020) or with analyses of organizational responses and other indirect measures of stakeholder attitudes instead of direct measures (Bentley, Oostman, & Shah, 2018; Gwebu et al., 2018; Kim et al., 2017; Kim & Lee, 2018; Wang & Park, 2017). Yet findings from the few studies directly connecting data breaches and stakeholder attitudes suggest that investing in stakeholder relationship development holds critical value for organizations who may experience these types of crises (Jahng & Hong, 2017; Janakiraman, Lim, & Rishika, 2018).

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 (2018) 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 (Diers-Lawson & Pang, 2016; Fuoli, van de Weijer, & Paradis, 2017), 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 (Coombs & Holladay, 2015; 2006; Johnston & Lane, 2018; Ma, 2018; Tao & Song, 2020; Yum & Jeong, 2014) and coupled with research demonstrating the impact stakeholder emotion invoked by the crisis itself (Cho & Gower, 2006; Diers-Lawson, 2017b; Jin, 2014; McDonald, Sparks, & Glendon, 2010; Schoofs, Claeys, De Waele, & Cauberghe, 2019), the question we should be broadly asking is what is the role of communication during security breaches?

We argue the focus should be directly on building an organization's capacity, which includes responding, managing, and serving stakeholder interests ahead of crisis (Heath, Lee, & Ni, 2009; Tao & Song, 2020). This approach highlights research findings that pre-crisis instructional messaging demonstrates strong impacts on people's behaviors and attitudes (Johnston & Lane, 2018; Sellnow, Johansson, Sellnow, & Lane, 2019; Zhou & Ki, 2018). As such, it becomes clear that the challenge of data breaches is as much a question of risk management or mitigation as it is post-crisis response. This view of data breaches is also aligned with Health and Millar's (2004) conceptualization of crises as untimely but predictable events. Therefore, the central aim of this paper is to explore the role of stakeholder attitudes and crisis communication in the context of data breaches to close the gaps in our knowledge.

Stakeholder Attitudes and Crisis Capacity

Strategic communication can be used to build capacity for managing crises; therefore, the stakeholder is and should always be the critical focus for any issues and crisis response (Diers-Lawson, 2020). Moreover, in the context of the data breach where it is the stakeholder's private information that has been compromised, the stakeholder's interests and concerns must be prioritized in order to manage the situation (e.g., Angst, et al., 2017; Choi, et al., 2016; IBM, 2019). Though stakeholder relationships differ from interpersonal ones (Coombs & Holladay, 2015), they can be characterized by pre-crisis relationship quality (Atkins & Lowe, 1994), the history of interaction with the organization (Jennings, Artz, Gillin, & Christodouloy, 2000), legitimate stakeholder interests in the data breach (Angst, et al., 2017), power the stakeholders have to affect the organization's success (IBM, 2019), and clear urgency to both address the material problems of the breach as well as stakeholder concerns (Janakiraman et al., 2018).

Stakeholder Relationship Management

As we discussed in the introduction, there is already unmistakable evidence of exponential growth in data breach cases globally (see Figure 1) and even greater risk because of the social distancing measures and move to more online work as a result of the COVID-19. Our core assumption is that stakeholder relationship management is vital to the successful resolution of data breaches. Thus, by adopting Diers-Lawson's (2020) stakeholder relationship model (SRM) as the core analytical model, we focus on the relationships between stakeholders, organizations, and the security of private data suggesting and posit that an organization's crisis capacity is likely as important as its direct response to a breach.

The Relationship Between the Issues and Organizations – Blame, Competence

Stakeholders make judgments about how organizations are connected to issues concerning them. Two of the most commonly cited judgements about the issue - organization relationship are judgments of the organization's competence to successfully manage the issue (Hyvärinen & Vos, 2015; Sohn & Lariscy, 2014), and of course whether they believe the organization should be blamed for the emergent crisis (Coombs, 2007; Schwarz, 2008).

Blame. Blame attribution is a core concept underlying different theories like situational crisis communication theory and it is applied in other crisis communication research connecting to other factors like corporate social responsibility, crisis history, and ethics (Kim, 2013; Ping, Ishaq, & Li, 2015). However, much of crisis communication theory conflates material blame and blame attribution. Material blame for a crisis is the degree to which organizations can be directly held accountable for a crisis (Rosati et al., 2019). This is why transgressions, or situations where direct blame is clearly attributable to the organization (Diers-Lawson, 2017a), tend to result in the greatest perceptions that the organization has betrayed the stakeholder's trust (Kim, Kim, & Cameron, 2009; Ma, 2018). Blame attribution, by comparison, represents the stakeholder's perception of the control the organization has over the issue (Weiner, 1985, 2006). Regardless of whether blame is perceptual or material, the more the crisis can be blamed on the organization, the higher the expectations placed on organizations to effectively manage the issue or crisis (Brown & Ki, 2013; Bundy & Pfarrer, 2015; Coombs, 2007). Previous research also suggests that higher perceptions of blame results in greater reputational damage for organizations (Coombs & Holladay, 1996; S. Kim, 2014; Schwarz, 2012) as well as negatively affecting behavioral intention towards

organizations in crisis (Ping et al., 2015; Yum & Jeong, 2014). However, Bentley, Oosman, and Shah (2018) point out that present theory building around crisis type struggles to account for contexts in which blame for the situation is more ambiguous, which is often the case with data breach crises. The result in these blame ambiguous crises, or organizational events (Diers-Lawson, 2017a), is that it is more difficult to provide tangible recommendations about crisis response strategy. This leads us to the conclusion that more clearly defining the context or situation, based on the information that would typically be a part of public discourse about a crisis will help us to better predict stakeholder reactions to organizational events like data breaches (Wang & Park, 2017); rather than merely assuming researcher and practitioner-based assumptions of blame attribution reflectingn on stakeholder evaluations. This is one of the reasons the present research looks beyond attribution-based theories in order to fully understand different situational factors that would affect the stakeholder, issue, and organizational dynamic. However, based on the strength of the previous research, we would predict that the level of blame will affect stakeholder evaluations and leaders to the following three hypotheses:

H1: Material blame will affect stakeholder evaluations of crisis response messages.
H2: Material blame will affect stakeholder behavioral intentions towards organizations.
H3: Material blame will affect the reputational threat generated by data breaches

Competence. Questions about how stakeholders assign blame to organizations have been asked since the 1970's with Schwartz and Ben David's (1976) analysis of blame, ability, and denial of responsibility in the face of emergencies. However, evaluations of an organization's competence in crisis response is, by contrast, a newer evolution in the field's understanding of the relationship between organizations and issues (Diers, 2012; Sohn & Lariscy, 2014). While competence has long been considered from an organization perspective, it has not always been considered from the stakeholder perspective. Competence asks whether stakeholders judge the organization has the capacity to successful resolve the problem (de Fatima Oliveira, 2013; Hyvärinen & Vos, 2015).

While there is evidence that competence in responding to and managing data breaches results in significantly lower costs for organizations facing them (IBM, 2019), there is also clear evidence that two-thirds of people report being less likely to shop or do business with an organization that has experienced a breach where financial or sensitive information was stolen (Graham, 2019). Though practitioner data points to clear outcomes, we lack clear theoretical connections to reconcile these two findings and predict how stakeholder evaluations of competence may influence outcomes to data breaches or how organizations can influence competence evaluations, reducing the value of making predictions about its impact. Therefore, we posit the following research question:

RQ1: Do stakeholder evaluations of an organization's competence to manage data breaches influence their attitudes about the organizations after a breach occurs?
RQ1A: Do stakeholder evaluations of an organization's competence to manage data breaches influence their evaluations of crisis response messages?
RQ1B: Do stakeholder evaluations of an organization's competence to manage data breaches influence their behavioral intention towards the organizations?

RQ1C: Do stakeholder evaluations of an organization's competence to manage data breaches influence the reputational threat generated by data breaches for organizations?

Stakeholders and Their Relationship to the Issue of Data Breaches

Stakeholder judgments about blame and competence are not made in a vacuum, they also come from stakeholder experiences and identities (Diers-Lawson, 2020). In the context of data security, previous research has found that individual attributes and attitudes shape privacy attitudes and data security behavioral intentions (Egelman & Peer, 2015). This view is well-aligned with research on attitude formation emphasizing the importance of constructs like perceived susceptibility, situation severity, demographics, and efficacy as key predictors of people's reactions to stimuli and situations (Chen, Gully, & Eden, 2001; Rosenstock, Strecher, & Becker, 1988). It is also well-aligned with research predicting that our behaviors can be accounted for by our existing attitudes, social norms, and perceived situational control (Ajzen, 2005). In fact, these findings also reflect research in crisis communication suggesting that stakeholder perceptions of their own control over issues and uncertainty about the situation affect not only their own emotional reactions to crises but attitudes and actions towards the organizations in crisis (Jin, Liu, Anagondahalli, & Austin, 2014; McDonald & Cokley, 2013; Mou & Lin, 2014).

Despite clear connections between the stakeholders, crises, and data breaches, there is little indication as to the role that stakeholders' attitudes and previous experiences with data security breaches would inform their reactions to crisis responses or their behavioral intentions towards organizations in crisis. One reason for this is that there are few direct measures of stakeholder attitudes on crisis response outside of the context of social media analyses. For example, studies like Kim, Johnson, and Park's (2017) analysis of five data breaches only looks at types of organizational responses, not stakeholder reactions to them. These descriptive studies are common in crisis communication research and have emerged in the first stage of research of data breaches (Bentley et al., 2018; Kim & Lee, 2018; Syed, 2019; Wang & Park, 2017); yet, it is important we continue to develop more sophisticated understandings of stakeholder factors. Therefore, we posit the following research question:

RQ2: How do stakeholders' attitudes towards data security breaches influence their attitudes about the organizations after a breach occurs?

RQ2A: How do stakeholders' attitudes towards data security breaches influence their evaluations of crisis response messages?

RQ2B: How do stakeholders' attitudes towards data security breaches influence their behavioral intention towards the organizations?

RQ2C: How do stakeholders' attitudes towards data security breaches influence the reputational threat generated by data breaches for organizations?

The Relationship Between Stakeholders and Organizations in Crisis

In the stakeholder relationship management model, the third major relationship to consider is the relationship between stakeholders and organizations in crisis (Diers-Lawson, 2020). One way theory in crisis communication has been developed is to examine the material impact of data breaches on consumer spending (e.g., Janakiraman, et al., 2018); however, the field needs to better understand the causal stakeholder attitudes underlying the behaviors to

improve predictive theory building. For example, research like Jahng and Hong's (2017) analysis applying social information processing theory to crisis response in data breaches found that prior brand attitude was a significant moderator in predicting purchase intentions. Across the existing industry and academic research on data breaches a consistent conclusion is that relationship management is a critical investment for any organization (*2019 Cost of a Data Breach Report*, 2019; Choi et al., 2016; Confente et al., 2019; Gwebu et al., 2018; Janakiraman et al., 2018; Syed, 2019).

Stakeholders' attitudes towards organizations in crisis have been studied extensively in crisis communication (Diers, 2012). However, these relationships focusing on reputation and trustworthiness are often treated as outcome variables instead of attributes of organizations. We would separate the concept of reputational damage or threat, which is a multi-step process that combines stakeholder evaluations of crisis severity and blame attribution with intensifiers like the organization's crisis history and its pre-crisis reputation (Diers-Lawson, 2020; Maresh & Williams, 2007; van Zoonen & van der Meer, 2015) as a distinctive concept from reputation and trustworthiness. Broadly, reputation represents stakeholder perceptions of an organization's appeal (Brown, Brown, & Billings, 2015), its social responsibility as a reflection of the organization's ethics (Bowen & Zheng, 2015), and its values (Falkheimer & Heide, 2015). And trustworthiness focuses on stakeholder evaluations of an organization's positive intent, behavior, and integrity (Mal, Davies, & Diers-Lawson, 2018; Mayer, Davis, & Schoorman, 1995; Shockley-Zalabak, Morreale, & Hackman, 2010). Because of the conflation of reputational threat and trustworthiness as outcomes versus pre-crisis reputation and trustworthiness as measurable factors contributing to how stakeholders make sense of crises, we would post the following research questions:

RQ3: How do stakeholder evaluations of an organization's reputation influence their attitudes about the organizations after a breach occurs?

RQ3B: How do stakeholder evaluations of an organization's reputation influence their evaluations of crisis response messages?

RQ3B: How do stakeholder evaluations of an organization's reputation influence their behavioral intention towards the organizations?

RQ3C: How do stakeholder evaluations of an organization's reputation influence the reputational threat generated by data breaches for organizations?

RQ4: How does an organization's trustworthiness influence stakeholder attitudes about the organizations after a breach occurs?

RQ4B: How does an organization's trustworthiness influence stakeholder evaluations of crisis response messages?

RQ4B: How does an organization's trustworthiness influence stakeholder behavioral intention towards the organizations?

RQ4C: How does an organization's trustworthiness influence stakeholder the reputational threat generated by data breaches for organizations?

Crisis Capacity, Data Breaches, and Communication

Since most research connecting stakeholders and data breaches is either descriptive or examines outcomes like final sales instead of stakeholder attitudes, there are insufficient studies to make more than weak hypotheses predicting a generic impact for each of the variables. What would be more useful in developing both theory and recommendations for

corporate communication practice is to place these relationships within the context of crisis capacity building (Diers-Lawson, 2020). Crisis capacity embraces Heath and Millar's (2004) notion that organizations should be the stewards of stakeholder interests and builds on Stacks (2004) multidimensional model of public relations. Stacks argues that effective crisis management focuses on three dimensions. First, an institutionalization of the corporate communications functions within organizations to build strong relationships with stakeholders helping to mitigate issues as they emerge, which improves decision-making, crisis response, and corporate strategy (Campiranon & Scott, 2014; Frandsen & Johansen, 2009; Miller & Horsley, 2009; Takamatsu, 2014). Second, considering the type of organization and customizing crisis response to build a consistent narrative that is both industry and organization-centered is essential for success (Bowen & Zheng, 2015; Kal-kausar, Rafida, Nurulhusna, Alina, & Mashitoh, 2013; Stacks, 2004). Third, effective crisis response develops specific and targeted messaging (Stacks, 2004; Steelman & McCaffrey, 2013). In an era where information seeking in crisis contexts is high and information sharing happens across platforms, it is certainly vital that organizations' engagement during data breaches is effective (Confente et al., 2019; Jahng & Hong, 2017; Vogler & Meissner, 2020; Wang & Park, 2017).

In addition to considering the influence of the relationships between organizations, stakeholders and issues as the stakeholder relationship model suggests, to understand the differences that can emerge in crisis capacity building between industries (e.g., Bowen & Zheng, 2015; Kalkausar, et al., 2013; Stacks, 2004) we also believe that a comparison between two of the industries that are most susceptible to data security breaches would provide richer information about crisis capacity building for data security. Therefore, we pose the following research question:

> *RQ5: Does the industry affected by the data security breach influence stakeholder attitudes about the organizations after a breach occurs?*
>
> > *RQ5A: Does the industry affected by the data security breach influence stakeholder evaluations of crisis response messages?*
> > *RQ5B: Does the industry affected by the data security breach influence stakeholder behavioral intentions towards the organizations?*
> > *RQ5C: Does the industry affected by the data security break influence reputational threat generated by data breaches for organizations?*

To summarize in brief, we propose the following conceptual model drawing together the stakeholder relationship management model and the consideration of industry (see Figure 2).

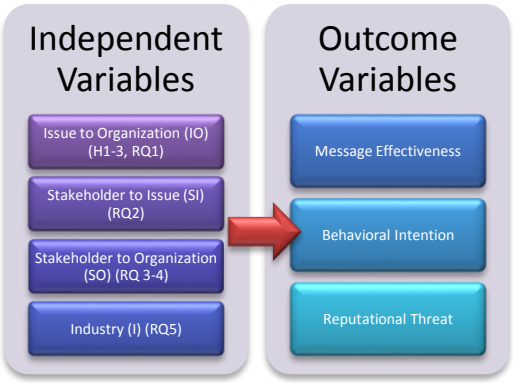

Figure 2. Conceptual Model for Study

Based on the study's design, we also propose the following overall research question:

RQ6: Which factors are most likely to affect organizations after a security data breach crisis?

RQ6A: Which factors best predict the success of a likely organizational response to data breaches?

RQ6B: Which factors best predict changes to stakeholders' behavioral intention after a data breach crisis?

RQ6C: Which factors best predict stakeholders' evaluation of reputational threat after a data breach crisis?

RQ6D: Controlling for factors influencing outcomes, how much influence does the crisis response message have on behavioral intention and reputational threat?

Methodology

To close the gaps in our knowledge, this study first establishes what a 'typical' organizational response to data breach is and then uses a 2 (material blame - organization at fault, organization not at fault) x 2 (type of organization – bank or primary health care provider) design with an additional control group (material blame - no crisis) in order to measure the impact of crisis capacity building as well as crisis response messages on public stakeholder behavioral intention.

Operationalizing the Type of Data Breach and Organizations

Previous research suggests there are three common types of data breach - criminal attacks, system glitches (i.e., technical errors), and human error. Instead of focusing on all three, we have focused on criminal attacks as being both the types of data breaches receiving the majority of media coverage with widespread reports over ransomware affecting global health, financial, and retail organizations and also because they are likely to generate the greatest issue engagement with stakeholders. In the coverage of criminal attacks, two types of material blame for organizations emerged – where organizations were warned about these cyberattacks and yet did not make changes in their systems ("NHS 'could have prevented' WannaCry ransomware attack," 2017) versus those organizations that can take measures to minimize or mitigate their risk to cyberattacks (O'Flaherty, 2018). To minimize the length of the questionnaire, we also used a control group design for the questionnaire instead of a pretest-posttest design.

Rather than focusing on a generic global response to data security breaches, because the experiment targeted British participants, cases of publicly reported data breaches in the UK, compiled by the company IT Governance UK, reported from January 2019-October 2019 were reviewed to identify the types of crisis response messages used by companies (N = 27) in order to identify the most culturally relevant responses since previous research has already identified there are likely to be cultural differences in crisis response (Kim & Lee, 2018). Of these 27 breaches, nine were attributable to user error or inappropriate data use within organizations, seven to technology failures, and 11 to criminal attack.

Organizational responses to these crises were coded based on Diers-Lawson's (2017a) typology of crisis response strategy to identify a typical 'British' response to data breaches which left personal information vulnerable to exploitation. Two independent coders analyzed

the responses with an 86% agreement on response coding. The analysis revealed that the most typical responses included accommodative (N = 8), framing the situation (N = 16), framing the organization (N = 6), excellence (N = 9), and interorganizational collaboration (N = 6) message strategies. One of the responses was selected and anonymized to represent a 'typical' response to data security breaches (see Appendix A).

Additionally, because data breaches focus on personal and private information being leaked like medical records and financial information and because both health organizations and financial organizations are consistent targets for cyberattacks (Graham, 2018, 2019; Irwin, 2020), we selected banks and primary health care providers as the types of organizations that would be used in the experiment. Brief scenarios were written (see Appendix B) to account for the 'situation' for respondents. Respondents were randomly assigned to the condition.

Manipulation Checks

The experiment's manipulation check was confirmed to be successful in two ways. The first was simply to identify whether participants understood the manipulation scenario. A Chi-square was used to identify the significance of the situation comprehension responses. In condition 1 – Bank, Material Blame 57 of 62 participants correctly recognized the summary of the situation (X^2 (3) = 148.19, $p < .00$). In condition 2 – GP (i.e., the British term for primary care physician or doctor's office), Material Blame 54 of 58 participants correctly recognized the summary of the situation (X^2 (2) = 98.55, $p < .00$). In condition 3 – Bank, No Material Blame, 60 of 66 participants correctly recognized the summary of the situation (X^2 (4) = 193.72, $p < .00$). In condition 4 – GP, No Material Blame 59 of 71 participants correctly recognized the summary of the situation (X^2 (3) = 127.93, $p < .00$). In condition 5 – Control 67 of 71 participants correctly recognized the summary of the situation (X^2 (3) = 182.24, $p < .00$).

The second way the manipulation check was confirmed was with a question after participants left the situation summary page to ensure they correctly remembered the situation by asking them, 'You have just read a statement about institutions that hold your private and secure information. To summarize the key theme, would you say this passage was primarily about…' and they selected the best response. A one-way ANOVA was run with the test condition as the independent variable and Scheffe post hocs confirming significant differences in the correct identification of each condition (F (4, 323) = 57.54, $p < .00$).

Sample

Participants were recruited through a snowball convenience approach resulting in 328 participants, 77% of whom lived in the UK (N = 252) and 23% (N = 76) either reported living outside of the UK or did not respond to that question. The sample was female biased with 61% (N = 200) self-identifying as female, 22.3% (N = 73) self-identifying as male, and 16.8% (N = 55) not responding or responding 'other'.

There was a reasonable distribution of participants based on age but with a slight bias with 1.5% (N = 4) representing people born from 1924-1945, 16.5% (N = 45) representing those born 1946-1964, 35.5% (N = 97) representing those born 1965-1979, 9.2% (N = 25) representing those born 1980-1994, and 37.4% (N = 102) representing those born 1995 and after, with 55 not responding to the question. Though not a representative sample, systematic

differences in the sample were balanced using a random assignment of participants to experimental groups.

The sample had a bias towards more affluent participants compared to the overall UK population (see Table 1 for the distribution). However, the sample is relatively representative of education levels in the UK with an overrepresentation of people with a bachelor's degree or post-graduate degrees (N = 128 or 47%) compared to the UK general population (40% BA, plus). However, participants with vocational degrees (N = 51 or 19%) and who have completed secondary education or college (N = 93 or 34%) are relatively similar to the UK general population.

Table I Summary of Sample Income Distribution, Compared to UK Population

Income	Sample Frequency	Sample Percent	UK Frequency[1]	UK Percent[1]
Less than £10,000	27	9.9	1767	3
£10,000-19,999	11	4.0	11593	18
£20,000-29,999	29	10.6	17312	27
£30,000-39,999	27	9.9	14162	22
£40,000-49,999	26	9.5	8161	13
£50,000-59,999	20	7.3	5448	8
£60,000-69,999	23	8.4	2617	4
£70,000-79,999	12	4.4	1369	2
£80,000-89,999	21	7.7	857	1
£90,000-99,999	25	9.2	460	1
Over £100,000	52	19.1	1427	2

Notes: [1]UK Frequency noted in thousands, from UK Office of National Statistics Data for 2019 available at: https://www.ons.gov.uk/peoplepopulationandcommunity/personalandhouseholdfinances/incomeandwealth/bulletins/householddisposableincomeandinequality/financialyearending2019#:~:text=Median%20household%20disposable%20income%20in,Living%20Costs%20and%20Food%20Survey.

Operationalization of Variables

The design controls for demographic factors (gender, age, income, education) and then analyses the relationship between the issue to organization (material blame and competence), stakeholder to issue (uncertainty avoidance, efficacy, data security behaviors, issue experience), stakeholder to organization (trustworthiness, reputation), and industry (medical or financial services) all evaluated as independent variables or control variables and crisis response statement effectiveness and behavioral intention (using the organization in the future and organizational support) used as key study variables.

Scales were evaluated using an exploratory principle components factor analysis (EFA)with a varimax rotation. Because most of the variables are being tested in new contexts and different populations, an EFA is more appropriate than a confirmatory factor analysis (CFA) because there is no hypothesized factor structure (Suhr, 2006). Once the factors were identified, Cronbach's alpha was used to test the reliability of the measures. Table 1 provides the operationalization, results of the factor analysis and Cronbach's alpha, relevant authors, and overall means for the variables.

Table II Operationalization of Study Variables, Descriptive Statistics

Variable	Author(s)	Mean	Eigen-value	Variance Explained	Factor Loading	Alpha
SI: Uncertainty Avoidance[1]	Jung & Kellaris, 2004	3.03	3.10	38.79		.82
SI: Efficacy	Chen, Gully, Eden, 2001	3.90	4.45	55.65		.88
SI: Security Behavior[2]: Software Updates	Egelman & Peer, 2015	2.93	4.15	34.60		.79
SI: Security Behavior[2]: Password Updates	Egelman & Peer, 2015	2.94	1.42	11.86		.74
Behavioral Intention: Use the organization	Ajzen, 1991	2.89	2.49	41.46		.76
Organizational Support	Ajzen, 1991	3.43	1.26	20.93		.66
Reputation Threat		3.81	4.38	54.76		.89
Based on this situation, how much damage would there be to the organisation's:						
Appeal					.64	
Competence					.76	
Social Responsibility					.78	
Trustworthiness					.85	
Reputation					.85	
Values					.71	
Credibility					.81	
SO: Trustworthiness	Morgan & Hunt, 1994	3.21	3.12	78.04		.91
SO: Reputation	Diers-Lawson, 2020; Diers, 2012; Walsh, Gianfranco, & Beatty, 2007	3.20	3.86	64.25		.89
IO: Data-Security Competence	Hargis & Watt, 2010; Jaques, 2009	3.11	1.97	65.55		.73
Crisis Response Statement Effectiveness		3.77	4.90	54.44		.90
The response is believable					.80	
The organisation clearly regrets what happened					.81	
The organisation will take all actions necessary					.80	
The statement was accommodating					.70	
The statement was socially responsible					.75	
The statement provided good information about the situation					.75	
The response was appropriate to the situation					.81	
The statement reflects well on the organisation					.80	
SI: Issue Experience – Others		1.92	1.50	37.49		.72
Do you know anyone who has been affected by a data breach?					.76	
Do you know anyone who has had a social media or email account hacked?					.82	
SI: Issue Experience – Personal		1.34	1.03	25.83		.73
Have you ever personally been affected by a data breach?					.87	
Have you ever had a social media or email account hacked?					.62	

[1]Resulted in 3-factor rotation, only 1 viable factor based on Cronbach's alpha
[2]Resulted in a 3-factor rotation, 2 viable factors based on Cronbach's alpha
[3]Resulted in a 4-factor rotation, 2 viable factors based on Cronbach's alpha

Data Analysis Methods

A combination of correlation with hierarchical regression and ANOVA with Scheffe post hoc analyses were used to analyze the data for each of the hypotheses and research questions, as appropriate.

Results

Overall, these data suggest that while organizations may use multi-layered messages to respond to data breaches, pre-crisis relationships with organizations are the principal factors that influence stakeholder attitudes about message, behavioral intent, and reputational threat. These results provide clear support for building a crisis capacity strategy for stakeholder relationship management to safeguard against negative outcomes for data breaches. This section will focus on the results for each of the relationships analyzed in turn.

Evaluating the Relationship Between the Issue and Organization After Data Breaches

Hypotheses 1, 2, and 3 and Research Question 1 evaluate the relationship between the issue (i.e., data breach) and the organization by evaluating the influence of material blame and competence in banks (B) compared the doctor's office (GP) on stakeholders' evaluation of message strategy and behavioral intention. ANOVAs were run to evaluate hypotheses 1 and 2. Correlations and simple regressions were run to answer RQ1.

H1-3 – The Effects of Material Blame on Message Evaluation and Outcomes

H1 proposing the material blame will affect message evaluation was supported. The ANOVA is significant (F (4, 273) = 3.79; p = .01) and the Scheffe post hoc (see Table II) reveals a significant difference between the control (M = 3.63) and GP with no material blame (M = 3.96), these data also reveal that across all conditions – including the control condition – that communicating an information-rich message highlighting competence, caring, cooperation, and the organization's identity is positively rated amongst stakeholders (M = 3.77). This suggests that as an approach to communicating about data security issues, practitioners using these types of talking points are judged as communicating effectively with stakeholders.

Table III ANOVA for the Impact of Material Blame on Message Evaluation and Outcomes

Dependent Variable	*df*	*F*	*p*	Post Hoc I	Post Hoc J	I-J	Sig.
Statement Effectiveness	4, 273	3.79	.01	GP, NM	C	.33	.03
Behavioral Intention – Use	4, 323	6.14	.00	B[1]M[5]	B, NM[4]	-.40	.03
the Organization					GP[2], NM	-.57	.00
					C	-.44	.01

Notes: The alpha for all tests was set at .05. Only significant differences in Post hocs reported
[1] B = Bank, [2] GP = Clinic, [3] C = Control Group, [4] NM = No Material Blame, [5] M = Material Blame

The ANOVA results support hypothesis 2 (F (4, 323) = 6.14; p = .00) that suggests material blame has influences on stakeholder behavior intentions. The results reveal there were differences in behavioral intention between industries (see Table III). In terms of behavioral intention to use the organization's services in the future, material blame mattered. The post hoc results demonstrate customers of banks who were aware of the threat and failed to act to prevent it are more likely to switch banks (M = 2.53). However, it was also found that the GP in the same situation (M = 2.87) was in a homogeneous subset with the banks at fault. That

does not mean that there is no risk even when organizations are not at fault or do not face a crisis. In fact, these data suggest that banks experiencing a data breach where they had the latest technology and were vigilant about security issues also have risk of losing customers (M = 2.93). Similarly, organizations not even in crisis but who discuss data security also face a mild threat of losing customers (M = 2.96). The only context where respondents indicated that there was no significant threat to losing 'customers' were GPs that could demonstrate proactive efforts to protect their patients' data (M = 3.09). Together, these data suggest that organizations discussing data breaches will be negatively affected regardless of whether a breach has happened directly to that organization. However, the magnitude and potential impact of that threat will depend on industry and material blame.

Hypothesis 3 was not supported; material blame had no significant influence on reputational threat.

RQ1– The Effects of Competence on Message Evaluation and Outcomes

These data suggest that stakeholder judgments of pre-crisis data security competence is critical in how they evaluate the effectiveness of an information-rich crisis response as well as their behavioral intention towards the organizations affected. Competence was significantly positively correlated to crisis response effectiveness (r (278) = .27; p =.00) , behavioral intention to use the organization (r (296) = .41; p =.00), and interest in showing support for the organization in crisis (r (296) = .26; p =.00). Moreover, all three simple regressions were significant as well indicating that pre-crisis data security competence significantly influences stakeholder perceptions of the crisis response statement effectiveness (β = .27; t (276) = 4.71; p = .00; $R^2_{adj.}$ = .07), their intention to use the organization after the crisis (β = .41; t (294) = 7.74; p = .00; $R^2_{adj.}$ = .17), and support they would be willing to show for the organization in crisis (β = .26; t (294) = 4.59; p = .00; $R^2_{adj.}$ = .06).

Evaluating the Relationship Between the Stakeholder and the Issue After Data Breaches

Research question 2 explores the influence of different, relevant, stakeholder attitudes on their evaluation of crisis response, behavioral intention towards organizations, and reputational threat. Data were analyzed using correlation and regression (where appropriate) to evaluate the influence of uncertainty avoidance, efficacy, data behaviors, and issue experience on the dependent variables. These data suggested that stakeholder attitudes about the issue has no influence on crisis response message effectiveness; therefore, RQ2A are not further reported.

For RQ2B exploring the relationship between stakeholder attitudes and behavioral intention, only personal data security behaviors (regular software updates) significantly predicted intention to continue using the organization with a significant correlation (r (328) = .12; p =.03) and significant simple regression (β = .12; t (326) = 2.24; p = .03; $R^2_{adj.}$ = .01). These data suggest that the relationship between the stakeholder and the issue itself is not a strong predictor for organizational outcomes after a data breach. However, stakeholder attitudes had no influence on support for the organization, so no further discussion is warranted.

For RQ2C exploring the relationship between stakeholder attitudes and reputational threat, there is a significant positive correlation between stakeholders' efficacy to protect themselves against data breaches and the reputational threat created by a data breach (r (328) = .11; p =.05) and also a significant simple regression (β = .11; t (326) = 2.01; p = .05; $R^2_{adj.}$ = .01).

Evaluating the Relationship Between the Stakeholder and the Organization After Data Breaches

Research questions 3 and 4 explore the relative influence of the organization's reputation and trust stakeholders place in the organization on their evaluation of crisis response messages, behavioral intention towards the organization after a crisis, and the reputational threat generated. Correlations and regressions (where appropriate) were used to analyze these data. These data demonstrate that reputation and trust significantly influence the dependent variables.

RQ3 measures the influence of reputation on crisis response statement effectiveness, behavioral intention, and reputational threat. Organizations facing data breaches with a reputation are significantly more likely to be effective in communicating about the situation with significant correlation (r (278) = .36; p =.00) and also a significant simple regression (β = .36; t (276) = 6.43; p = .00; $R^2_{adj.}$ = .13). A positive reputation also influences stakeholder intention to use the organization after the crisis with significant correlation (r (296) = .54; p =.00) and also a significant simple regression (β = .54; t (294) = 11.02; p = .00; $R^2_{adj.}$ = .29). Similarly a positive reputation also encourages stakeholders to demonstrate more support for the organization after the crisis with significant correlation (r (296) = .36; p =.00) and also a significant simple regression (β = .36; t (294) = 6.55; p = .00; $R^2_{adj.}$ = .12). Finally, a positive reputation encourages stakeholders to believe the organization will suffer less reputational threat after the crisis with significant correlation (r (296) = -.17; p =.00) and also a significant simple regression (β = .-.17; t (294) = -2.94; p = .00; $R^2_{adj.}$ = .03).

RQ4 measures the influence of stakeholder trust in the organization on crisis response statement effectiveness, behavioral intention, and reputational threat. When stakeholders trust the organization facing a data breach the organization's response to the situation is significantly more likely to be effective (r (278) = .28; p =.00) and also a significant simple regression (β = .27; t (276) = 4.78; p = .00; $R^2_{adj.}$ = .08). Stakeholder trust also influences their intention to use the organization after the crisis with significant correlation (r (296) = .51; p =.00) and also a significant simple regression (β = .51; t (294) = 10.27; p = .00; $R^2_{adj.}$ = .26). Similarly stakeholder trust also encourages stakeholders to demonstrate more support for the organization after the crisis with significant correlation (r (296) = .32; p =.00) and also a significant simple regression (β = .32; t (294) = 5.77; p = .00; $R^2_{adj.}$ = .10). Finally, stakeholder trust leads to their belief that the organization will suffer less reputational threat after the crisis with significant correlation (r (296) = -.21; p =.00) and also a significant simple regression (β = .-.21; t (294) = -3.64; p = .00; $R^2_{adj.}$ = .04).

Evaluating the Influence of Industry on Stakeholder Attitudes After a Data Breach

Research question 5 explores the influence of the industry alone on stakeholder evaluations of crisis response messages, behavioral intention, and reputational damage after data breach crises in order to evaluate risks for data breaches in public versus private industries. ANOVA was used to analyze the influence of industry.

RQ5A asked whether industry would influence stakeholder attitudes about the effectiveness of an information rich crisis response statement. The findings suggest that industry has a significant influence on crisis response statement effectiveness (F (2, 275) = 3.19; p = .04) with post hocs (see Table IV) revealing that doctor's offices experiencing data breaches would be significantly more effective (M = 3.86) compared to the control group (M = 3.63).

These data also found for RQ5B that behavioral intention was significantly influenced by industry. Intention to use the organization after the data breach was significantly different (F (2, 325) = 4.90; p = .01) depending on industry with stakeholders significantly less likely to use banks (M = 2.73) compared to their doctor's offices (M = 2.99) if they experienced a data breach (see Table III). Additionally, stakeholders felt significantly different supporting organizations in different industries experiencing data security breaches (F (2, 325) = 10.87; p = .00) with post hocs indicating (see Table IV) that they were significantly less likely to support banks (M = 3.20) compared to both their doctor's offices (M = 3.52) and the control group (M = 3.66) in data security crises. There were, however, no significant differences for RQ5C identifying differences in the levels of perceived reputational threat across the industries.

Table IV ANOVA for Industry Impact on Outcome Variables

Dependent Variable	*df*	*F*	*p*	Post Hoc I	Post Hoc J	I-J	Sig.
Crisis Response Statement Effectiveness	2, 275	3.19	.04	GP	C	.23	.04
Behavioral Intention -Use the Organization	2, 325	4.90	.01	Bank	GP	-.26	.01
Behavioral Intention - Statement Effectiveness	2, 325	10.87	.00	Bank	GP	-.32	.00
				Bank	Control	-.46	.00

Notes: The alpha for all tests was set at .05. Only significant differences in Post hocs reported
B = Bank, GP = Clinic, C = Control Group,

Evaluating the Overall Factors Affecting Organizations Facing Data Security Breaches

These individual findings provide insight into the factors influencing stakeholder evaluations of organizations facing data security breaches. However, when these factors are considered in research question 6, the clear finding is that building crisis capacity before a crisis provides organizations facing data security breaches the best opportunity to be persuasive and maintain a positive relationship with their stakeholders. Data were analyzed together in a hierarchical regression and include demographic control variables (where significantly correlated) of gender, age, income, and education.

RQ6A – Factors Influencing Crisis Response Effectiveness

Based on significant correlations previously discussed, the issue to organization and stakeholder to organization relationships were evaluated in a two-model hierarchical regression to evaluate the factors influencing the effectiveness of information rich crisis response messages to data security breaches. Both model 1 (F (2, 274) = 11.65; p = .00) and model 2 (F (5, 272) = 12.13; p = .00) were significant with a total adjusted r-square of .17 (see Figure 3). Notably, a preventative crisis message is significantly less likely to be effective, accounting for about 11% of the variance alone suggesting organizations should not attempt to communicate about data breaches before they happen. Therefore, in model 2 only a positive pre-crisis reputation significantly predicted the success of the crisis response strategy.

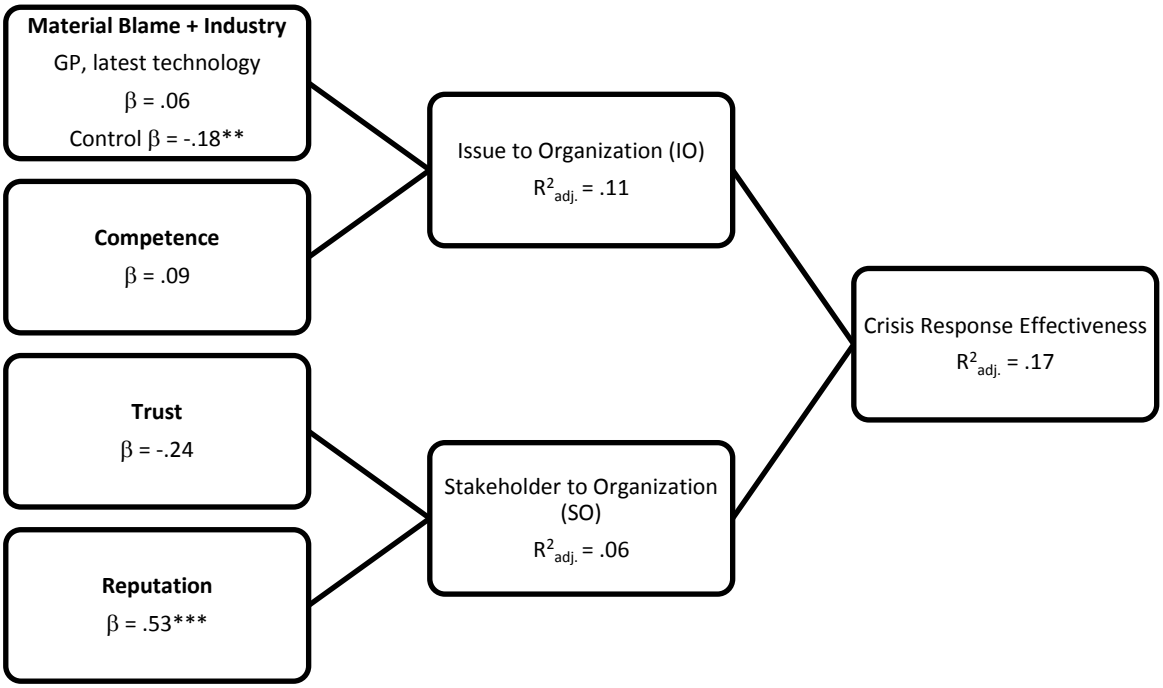

Figure 3. RQ6A Findings

RQ6B – Factors Influencing Stakeholders' Intention to Use the Organization Post-Crisis
Based on significant correlations previously discussed, the issue to organization, stakeholder to issue, and stakeholder to organization relationships were evaluated in a three-model hierarchical regression to evaluate the factors influencing stakeholders' behavioral intention to organizations experiencing data security breaches. Model 1 (F (3, 292) = 24.81; p = .00), model 2 (F (4, 291) = 19.79; p = .00), and model 3 (F (6, 289) = 22.34; p = .00) were significant with a total adjusted r-square of .30 (see Figure 4). However, in model 3 only a positive pre-crisis reputation significantly predicted stakeholders' intention to use the organization facing the data security breach after the crisis.

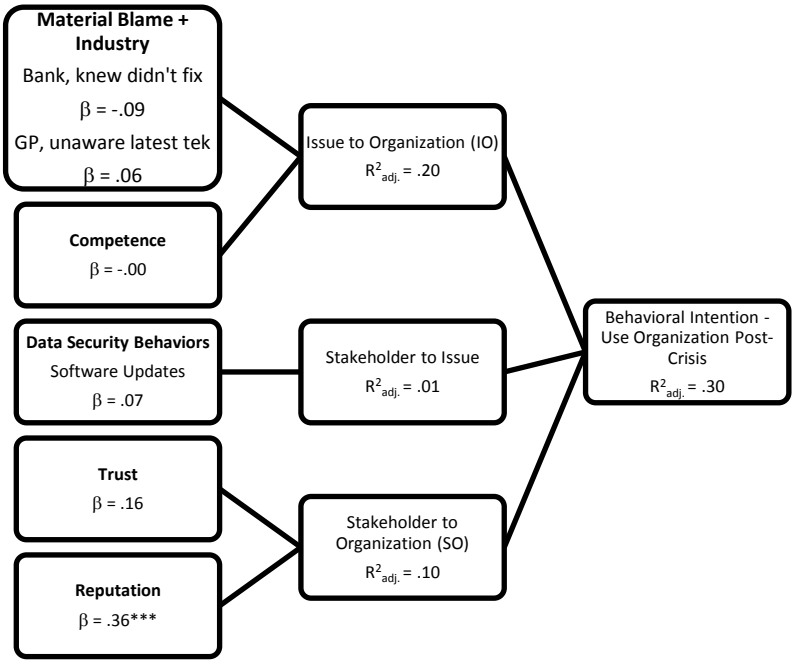

Figure 4. RQ6B Findings

RQ6C – Factors Influencing Stakeholders' Perception of Reputational Threat Post-Crisis

Based on significant correlations previously discussed, issue to organization, stakeholder to issue, and stakeholder to organization relationships were evaluated in a three-model hierarchical regression to evaluate the factors influencing stakeholders' perception of reputational threat to organizations facing a data security breach. Gender was also significantly correlated (r (273) = .13; p = .04) and was included as a control variable, though it had no effect in the final model. Model 1 (F (3, 269) = 8.78; p = .00), model 2 (F (4, 268) = 8.45; p = .00), and model 3 (F (6, 266) = 5.83; p = .00) were significant with a total adjusted r-square of .10 (see Figure 5). In the final model, both issue to organization and stakeholder to issue evaluations were significant. The majority of the variance ($R^2_{adj.}$ = .07) was accounted for by the negative relationship between the organization's competence on data security issues and reputational threat; however, stakeholder pre-existing efficacy also significantly influenced reputational threat with a positive relationship between efficacy and reputational threat.

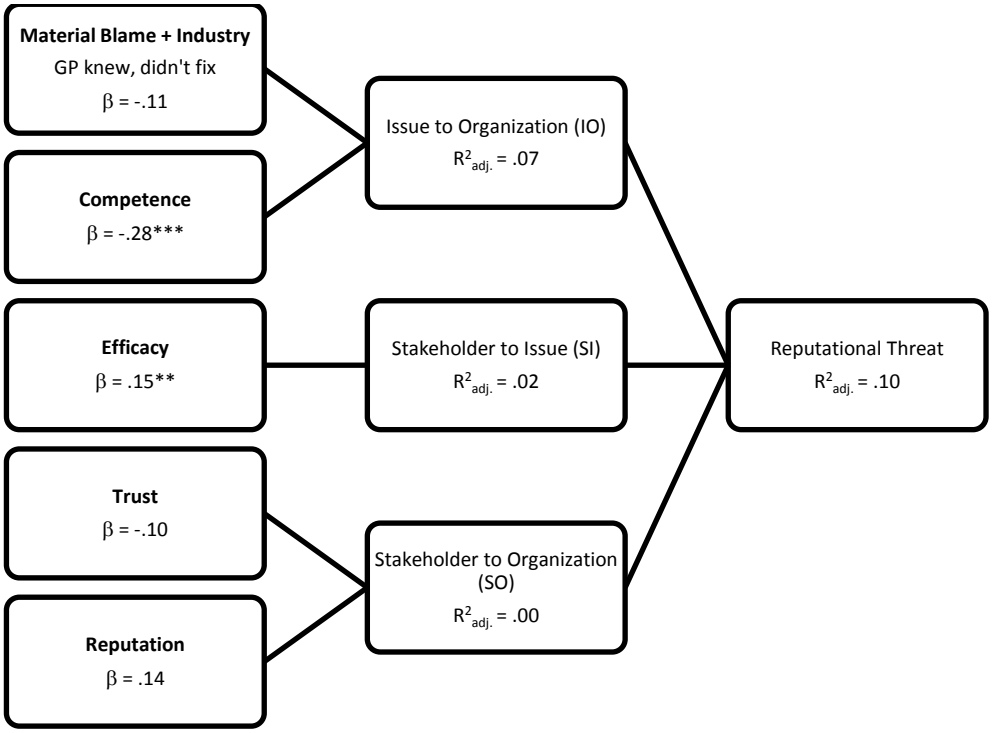

Figure 5. RQ6C Findings

RQ6D – The Influence of Crisis Response Messages on Data Breach Outcomes

In order to isolate the influence of post-crisis messages on stakeholders' intention to use the organization in crisis after the breach and their perceptions of the reputational threat posed by the crisis, a two-model hierarchical regression was used for each of the dependent variables. In evaluating the influence of post-crisis messages on stakeholders' intention to use the organization after a crisis both model 1 (F (6, 271) = 22.17; p = .00, $R^2_{adj.}$ = .31) and model 2 (F (7, 270) = 19.24; p = .00, $R^2_{adj.}$ = .31) were significant. However, in the second model the crisis response message (β = .07) was not significant and did not significantly change the r-square adjusted indicating that the previous model emphasizing the importance of pre-crisis reputation was the most robust.

In evaluating the influence of post-crisis messages on stakeholders' perception of the data security breach's threat to the organization's reputation, crisis response messages did significantly influence their appraisal. Both model 1 (F (5, 272) = 5.81; p = .00, $R^2_{adj.}$ = .08) and model 2 (F (6, 271) = 5.75; p = .00, $R^2_{adj.}$ = .09) were significant. In the second model the crisis response message was significant (β = .14, p = .03); however, the more effectively the organization communicated an information rich message about the crisis, the greater stakeholders evaluated the risk of the crisis to the organization's reputation.

Discussion and Conclusions

One of the principle weaknesses in previous research was that while we have several analyses of how organizations respond in data breaches, we know little about how the situation may affect stakeholders' behavioral intention and evaluations of the message's effectiveness (Jahng & Hong, 2017; Janakiraman, Lim, & Rishika, 2018). Broadly the field of communication assumes that getting the right message to the right audience at the right time will create more positive outcomes for organizations. For the last several decades much of the field of crisis communication has assumed that in the context of a crisis the response strategy itself would materially help the organization. In fact, many of the studies of crisis communication from 1953 to 2014 emphasized identifying what crisis response strategies that organizations use to engage stakeholders after a crisis has emerged (Diers-Lawson, 2020; 2017a). Though there are limited crisis communication studies of data breaches, these studies have often followed this approach in describing organizational responses to the data breaches (e.g., Kim, et al., 2017; Kim & Lee, 2018; Wang & Park, 2017).

Because of this assumption, predictive theory has been difficult to develop, as evidenced by the research gaps we discussed both in relation to data security breaches and more broadly earlier in the paper (see e.g., Bakker, et al., 2018). Though these data are specific to both the UK and data security breaches in two industries, these findings should make the field question the primacy of crisis response strategies compared to building more resilient organizations (see, e.g., Doerfel, et al., 2020) or building crisis capacity. These data suggest that reactive crisis response may have limited predictive value once we consider the relationships between organization, the issue, and stakeholders. To validate this finding, future research should explore more representative samples, additional national contexts, industries, and types of crises; however, we believe this helps to better explain some of the limitations in research and practice of excellence in crisis response not translating immediately into reputational gains (see, e.g., Diers-Lawson & Pang, 2016; Diers, 2012).

We recognize this is a bold conclusion; however, we believe the data clearly leads us to this conclusion. This project controlled the type of crisis situation, focused on a culturally relevant response, and used not only the most common crisis response strategy within that cultural context, but also one that previous research has identified ought to be used (across cultural contexts), and found that the response was viewed favorably. Despite all of that, there was no significant impact for a culturally relevant and favorable crisis response message on stakeholder behavioral intention once other factors – particularly reputation and issue competence – were considered. Of course, these findings are limited by a very specific type of a situation (i.e., data breaches), in a specific cultural context (i.e., the UK), in limited industries (i.e., banking and healthcare), and was based on data that was not entirely representative of the whole population, but we argue these findings are strong enough to warrant broadening the scope of the study to other contexts. These findings are also limited in

their application to short-term behavioral intention and do not reflect long-term impact of communicating effectively and ethically after a crisis.

The long-term impacts of stakeholder engagement are also reflected in these findings. While these data suggest that reactive crisis response has little impact on immediate behavioral intention, these data also suggest that evaluations of the right time for stakeholder engagement are in the periods where organizations are not in crisis. However, these findings also offer a strong data security caveat – heightening stakeholders' perceptions of risk for data breaches are likely to be counterproductive. More specifically, in our control group, there was no data breach; however, we reminded them that organizations hold private information and any organization may be susceptible to an illegal data breach (see Appendix B). A message like this is common across many types of institutions with secure log-ins and is designed to be a neutral message. However, these messages may damage both behavioral intent and generate reputation threat because they change the risk level without providing a solution to the problem (see Witte, 1996). Future research should explore this efficacy dynamic with data security breaches further. Instead, these data support previous research suggesting that a strong pre-crisis reputation is a vital part of building an organization's crisis capacity to minimize negative behavioral intention after a crisis (Jahng & Hong, 2017; Tao & Song, 2020).

The findings also suggest that stakeholder's judgments of an organization's competence to deal with a specific type of crisis – in our case the data breach – is likely tied to their attitudes about the organization that exist before the crisis emerges as well. In their conceptual piece Coombs and Holladay (2015) posited that social responsibility might well represent a risk to organizations once a crisis breaks. However, these findings along with others (Bae, Choi, & Lim, 2020; Kim & Lee, 2015; Tao & Song, 2020; Zhou & Ki, 2018) all suggest that organizations can build crisis capacity through long-term relationship development, demonstration of good will, trustworthiness – in short, the work that public relations in ethical organizations should be doing on a regular basis – represents a meaningful buffer against crises no matter the situational factors. Importantly, these findings also support and provide good theoretically grounded explanations for applied research identifying that organizations that are prepared and respond well can literally save themselves millions when facing data breaches (*2019 Cost of a Data Breach Report*, 2019; Gwebu et al., 2018).

In applying Diers (2012) stakeholder relationship model, this study examined the two paths most crisis research takes – the first focusing on the organization and organizational responses to crisis and the second focusing on the organization's capacity to respond. These data suggest that reactive crisis response has limited impact on stakeholder behavioral intentions once the factors that influence crisis capacity building are considered. However, without a strong relationship between an organization and its stakeholders ahead of a crisis, even the best responses are unlikely to help the organization in the short-term. These data also demonstrate that, at least within a British context, information-rich messages that highlight the organization's competence, caring, cooperation, and the organization's identity are well-received messages that reinforce the stakeholder's perception when they have a positive view of the organization to begin with.

For practitioners, these findings provide a compelling argument for the investment in long-term relationship development and management with an organization's existing stakeholders, independent of marketing efforts, as crisis capacity building activities. If the exponential growth in the last few years in data breaches tells us anything, it is that crises are inevitable

and if organizations are to retain their existing stakeholders let alone develop new ones, they must demonstrate their goodwill, trustworthiness, and competence before the crisis occurs. Afterwards, it may be too late to minimize the loss of business and patronage.

References

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

Ajzen, I. (2005). *Explaining intentions and behavior: Attitudes, personality, and behavior* (Vol. 2nd). Berkshire, England: McGraw-Hill Education.

Angst, C. M., Block, E. S., D'arcy, J., & 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), 893-916.

Atkins, M., & Lowe, J. (1994). Stakeholders and the strategy formation process in small and medium enterprises. *International Small Business Journal, 12*(3), 12-25.

Bae, J., Choi, W., & Lim, J. (2020). Corporate social responsibility: An umbrella or a puddle on a rainy day? Evidence surrounding corporate financial misconduct. *European Financial Management, 26*(1), 77-117. doi:https://doi.org/10.1111/eufm.12235

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*(2), 277-286. doi:ps://doi.org/10.1016/j.pubrev.2018.02.004

Bentley, J. M., Oostman, K. R., & Shah, S. F. A. (2018). We're sorry but it's not our fault: Organizational apologies in ambiguous crisis situations. *Journal of Contingencies and Crisis Management, 26*(1), 138-149. doi:https://doi.org/10.1111/1468-5973.12169

Bowen, S. A., & Zheng, Y. (2015). Auto recall crisis, framing, and ethical response: Toyota's missteps. *Public Relations Review, 41*(1), 40-49. doi:http://dx.doi.org/10.1016/j.pubrev.2014.10.017

Brown, K. A., & Ki, E.-J. (2013). Developing a valid and reliable measure of organizational crisis responsibility. *Journalism & Mass Communication Quarterly, 90*(2), 363-384. doi:10.1177/1077699013482911

Brown, N. A., Brown, K. A., & Billings, A. C. (2015). "May No Act of Ours Bring Shame" Fan-Enacted Crisis Communication Surrounding the Penn State Sex Abuse Scandal. *Communication & Sport, 3*(3), 288-311. doi:10.1177/2167479513514387

Bundy, J., & Pfarrer, M. D. (2015). A burden of responsibility: The role of social approval at the onset of a crisis. *Academy of Management Review, 40*(3), 345-369. doi:http://dx.doi.org/10.5465/amr.2013.0027

Campiranon, K., & Scott, N. (2014). Critical success factors for crisis recovery management: A case study of Phuket hotels. *Journal of Travel & Tourism Marketing, 31*(3), 313-326. doi:10.1080/10548408.2013.877414

Chen, G., Gully, S. M., & Eden, D. (2001). Validation of a new general self-efficacy scale. *Organizational Research Methods, 4*(1), 62-83.

Cho, S. H., & Gower, K. K. (2006). Framing effect on the public's response to crisis: Human interest frame and crisis type influencing responsibility and blame. *Public Relations Review, 32*(4), 420-422.

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.

Claeys, A.-S., & Cauberghe, V. (2015). The role of a favorable pre-crisis reputation in protecting organizations during crises. *Public Relations Review, 41*(1), 64-71. doi:10.1016/j.pubrev.2014.10.013

Claeys, A.-S., Cauberghe, V., & Vyncke, P. (2010). Restoring reputations in times of crisis: An experimental study of the Situational Crisis Communication Theory and the moderating effects of locus of control. *Public Relations Review, 36*(3), 256-262. doi:10.1016/j.pubrev.2010.05.004

Clementson, D. E. (2020). Narrative persuasion, identification, attitudes, and trustworthiness in crisis communication. *Public Relations Review*, in press. doi:https://doi.org/10.1016/j.pubrev.2020.101889

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*(4), 492-504. doi:https://doi.org/10.1016/j.emj.2019.01.007

Coombs, T., & Holladay, S. (2015). CSR as crisis risk: expanding how we conceptualize the relationship. *Corporate Communications: An International Journal, 20*(2), 144-162. doi:http://dx.doi.org/10.1108/CCIJ-10-2013-0078

Coombs, T. W., and Holladay, S. J. (2006). Unpacking the halo effect: reputation and crisis management. *Journal of Communication Management*, 10(2), 123-137.

Coombs, W. T. (2006). The protective powers of crisis response strategies: Managing reputational assets during a crisis. *Journal of Promotion Management, 12*(3/4), 241-260. doi:10.1300/J057v12n03•13

Coombs, W. T. (2007). Attribution theory as a guide for post-crisis communication research. *Public Relations Review, 33*(2), 135-139.

Coombs, W. T., & Holladay, S. J. (1996). Communication and attributions in a crisis: An experimental study in crisis communication.

Journal of Public Relations Research, 8(4), 279-295.

Coombs, W. T., & Holladay, S. J. (2015). Public relations'"relationship identity" in research: Enlightenment or illusion. *Public Relations Review, 41*(5), 689-695. doi:http://dx.doi.org/10.1016/j.pubrev.2013.12.008

De Bruycker, I., & Walgrave, S. (2014). How a new issue becomes an owned issue. Media coverage and the financial crisis in Belgium (2008–2009). *International Journal of Public Opinion Research, 26*(1), 86-97.

de Fatima Oliveira, M. (2013). Multicultural environments and their challenges to crisis communication. *Journal of Business Communication*, 0021943613487070. doi:10.1177/0021943613487070

Diers-Lawson, A. (2017a). Crisis CommunicationOxford Research Encyclopedia of Communication: Oxford University Press. Retrieved from http://communication.oxfordre.com/view/10.1093/acrefore/9780190228613.001.0001/acrefore-9780190228613-e-397. doi:10.1093/acrefore/9780190228613.013.397

Diers-Lawson, A. (2017b). Will They Like Us When They're Angry? Antecedents and Indicators of Strong Emotional Reactions to Crises Among Stakeholders. In S. M. Croucher, B. Lewandowska-Tomaszczyk, & P. Wilson (Eds.), *Conflict, mediated message, and group dynamics* (pp. 81-136). Lanham, MD: Lexington Books.

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

Diers-Lawson, A., & Pang, A. (2016). Did BP Atone for its Transgressions? Expanding Theory on 'Ethical Apology'in Crisis Communication. *Journal of Contingencies and Crisis Management, 24*(3), 148-161.

Diers, A. R. (2012). Reconstructing stakeholder relationships using 'corporate social responsibility' as a response strategy to cases of corporate irresponsibility: The case of the 2010 BP spill in the Gulf of Mexico. In R. Tench, W. Sun, & B. Jones (Eds.), *Corporate Social Irresponsibility: A Challenging Concept* (Vol. 4, pp. 177-206). United Kingdom: Emerald.

Egelman, S., & Peer, E. (2015). Predicting privacy and security attitudes. *Computers and Society, 45*(1), 22-28. doi:https://doi.org/10.1145/2738210.2738215

Falkheimer, J., & Heide, M. (2015). Trust and Brand Recovery Campaigns in Crisis: Findus Nordic and the Horsemeat Scandal. *International Journal of Strategic Communication, 9*(2), 134-147. doi:10.1080/1553118X.2015.1008636

Frandsen, F., & Johansen, W. (2009). Institutionalizing crisis communication in the public sector: An explorative study in Danish municipalities. *International Journal of Strategic Communication, 3*(2), 102-115.

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*(4), 645-660. doi:https://doi.org/10.1016/j.pubrev.2017.07.007

Graham, A. (2018). Infographic: List of data breaches in 2017.

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

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*(2), 683-714.

Haley, E. (1996). Exploring the construct of organization as source: Consumers' understandings of organizational sponsorship of advocacy advertising. *Journal of advertising, 25*, 19-36.

Heath, R., Lee, J., & Ni, L. (2009). Crisis and risk approaches to emergency management planning and communication: The role of similarity and sensitivity. *Journal of Public Relations Research, 21*(2), 123-141. doi:10.1080/10627260802557415

Heath, R. L., & Millar, D. P. (2004). A Rhetorical Approach to Crisis Communication: Management, Communication Processes, and Strategic Responses. In D. P. Millar & R. L. Heath (Eds.), *Responding to Crisis: A Rhetorical Approach to Crisis Communication* (pp. 1-18). Mahwah, NJ: Lawrence Erlbaum Associates.

Hong, S., Yang, S., & Rim, H. (2010). The influence of corporate social responsibility and customer–company identification on publics' dialogic communication intentions. *Public Relations Review, 36*(2), 196-198. doi:10.1016/j.pubrev.2009.10.005

Huang, Y. (2008). Trust and relational commitment in corporate crises: The effects of crisis communicative strategy and form of crisis response. *Journal of Public Relations Research, 20*(297-327).

Hyvärinen, J., & Vos, M. (2015). Developing a conceptual framework for investigating communication supporting community resilience. *Societies, 5*(3), 583-597. doi:10.3390/soc5030583

Irwin, L. (2020, March 9, 2020). Infographic: Cyber attacks and data breaches of 2019.

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*(2), 147-157. doi:10.1057/s41299-017-0022-7

Janakiraman, R., Lim, J. H., & Rishika, R. (2018). The effect of a data breach announcement on customer behavior: Evidence from a multichannel retailer. *Journal of marketing, 82*(2), 85-105. doi:https://doi.org/10.1509/jm.16.0124

Jennings, D. F., Artz, K., Gillin, L. M., & Christodouloy, C. (2000). Determinants of trust in global strategic alliances: Amrad and the Australian biomedial industry. *Competitiveness Review, 10*(1), 25-44.

Jin, Y. (2014). Examining publics' crisis responses according to different shades of anger and

sympathy. *Journal of Public Relations Research, 26*(1), 79-101. doi:10.1080/1062726X.2013.848143

Jin, Y., Liu, B. F., Anagondahalli, D., & Austin, L. (2014). Scale development for measuring publics' emotions in organizational crises. *Public Relations Review, 40*(3), 509-518. doi:http://dx.doi.org/10.1016/j.pubrev.2014.04.007

Johnston, K. A., & Lane, A. B. (2018). Building relational capital: The contribution of episodic and relational community engagement. *Public Relations Review, 44*(5), 633-644. doi:https://doi.org/10.1016/j.pubrev.2018.10.006

Kal-kausar, M., Rafida, A. N., Nurulhusna, N., Alina, A., & Mashitoh, A. S. (2013). Crisis Communication and Management on Food Recall in the Malaysian Food Industry. *Middle-East Journal of Scientific Research, 13*, 54-60. doi:10.5829/idosi.mejsr.2013.16.s.100210

Ki, E.J., & Brown, K. A. (2013). The effects of crisis response strategies on relationship quality outcomes. *Journal of Business Communication, 50*(4), 403-420. doi:10.1177/0021943613497056

Kim, B., Johnson, K., & Park, S.Y. (2017). Lessons from the five data breaches: Analyzing framed crisis response strategies and crisis severity. *Cogent Business & Management, 4*(1), 1354525.

Kim, H.S., & Lee, S. Y. (2015). Testing the Buffering and Boomerang Effects of CSR Practices on Consumers' Perception of a Corporation during a Crisis. *Corporate reputation review, 18*(4), 277-293. doi:10.1057/crr.2015.18

Kim, J., Kim, H. J., & Cameron, G. T. (2009). Making nice may not matter: The interplay of crisis type, response type and crisis issue on perceived organizational responsibility. *Public Relations Review, 35*(1), 86-88.

Kim, N., & Lee, S. (2018). Cybersecurity breach and crisis response: An analysis of organizations' official statements in the United States and South Korea. *International Journal of Business Communication*, 2329488418777037. doi:https://doi.org/10.1177/2329488418777037

Kim, S. (2013). Corporate ability or virtue? Relative effectivenss of prior corporate associations in times of crisis. *International Journal of Strategic Communication, 7*(4), 241-256. doi:10.1080/1553118X.2013.824886

Kim, S. (2014). The role of prior expectancies and relational satisfaction in crisis. *Journalism & Mass Communication Quarterly, 91*(1), 139-158. doi:10.1177/1077699013514413

Lacey, R., Kennett-Hensel, P. A., & Manolis, C. (2015). Is corporate social responsibility a motivator or hygiene factor? Insights into its bivalent nature. *Journal of the Academy of Marketing Science, 42*(3). doi:10.1007/s11747-014-0390-9

Ma, L. (2018). How to turn your friends into enemies: Causes and outcomes of customers' sense of betrayal in crisis communication. *Public Relations Review, 44*(3), 374-384. doi:https://doi.org/10.1016/j.pubrev.2018.04.009

Mal, C. I., Davies, G., & Diers-Lawson, A. (2018). Through the looking glass: The factors that influence consumer trust and distrust in brands. *Psychology & Marketing, 35*(12), 936-947.

Maresh, M., & Williams, D. (2007). *Toward an industry-specific crisis response model: A look at the oil crises of British Petroleum and Phillips Petroleum*. Paper presented at the National Communication Association, Chicago, IL.

Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An integrative model of organizational trust. *Academy of Management Review, 20*(3), 709-734.

McDonald, L. M., & Cokley, J. (2013). Prepare for anger, look for love: A ready reckoner for crisis scenario planners. *PRism, 10*(1), 1-11.

McDonald, L. M., Sparks, B., & Glendon, A. I. (2010). Stakeholder reactions to company crisis communication and causes. *Public Relations Review, 36*(3), 263-271.

Miller, B. M., & Horsley, J. S. (2009). Digging deeper: Crisis management in the coal industry. *Journal of Applied Communication Research, 37*(3), 298-316.

Mou, Y., & Lin, C. A. (2014). Communicating Food Safety via the Social Media The Role of Knowledge and Emotions on Risk Perception and Prevention. *Science Communication, 36*(5), 593-616. doi:10.1177/1075547014549480

NHS 'could have prevented' WannaCry ransomware attack. (2017). *BBC News: Technology*. Retrieved from BBC News website: https://www.bbc.co.uk/news/technology-41753022

O'Flaherty, K. (2018). How to survive a ransomware attack -- and not get hit again. *Forbes: Innovation*. Retrieved from Forbes.com website: https://www.forbes.com/sites/kateoflahertyuk/2018/08/17/how-to-survive-a-ransomware-attack-and-not-get-hit-again/#3bc64af06cd3

Oles, D. L. (2010). Deny, delay, apologize: The Oprah Winfrey image-defense playbook. *Northwest Journal of Communication, 39*(1), 37-63.

Ping, Q., Ishaq, M., & Li, C. (2015). Product Harm Crisis, Attribution of Blame and Decision Making: An Insight from the Past. *Journal of Applied Environmental and Biological Sciences, 5*(5), 35-44.

Piotrowski, C., & Guyette, R. W. (2010). Toyota recall crisis: Public attitudes on leadership and ethics. *Organizational Development Journal, 28*(2), 89-97.

Rosati, P., Deeney, P., Cummins, M., Van der Werff, L., & Lynn, T. (2019). Social media and stock price reaction to data breach announcements: Evidence from US listed companies. *Research in International Business and Finance, 47*, 458-469. doi:https://doi.org/10.1016/j.ribaf.2018.09.007

Rosenstock, I. M., Strecher, V. J., & Becker, M. H. (1988). Social learning theory and the health belief model. *Health Education and Behavior, 15*(2), 175-183. doi:10.1177/109019818801500203

Samkin, G., Allen, C., & Wallace, K. (2010). Repairing Organisational Legitimacy: the Case of the New Zealand Police. *Australasian Accounting Business & Finance Journal, 4*(3), 23-45. doi:2170715441

Schoofs, L., Claeys, A.-S., De Waele, A., & Cauberghe, V. (2019). The role of empathy in crisis communication: Providing a deeper understanding of how organizational crises and crisis communication affect reputation. *Public Relations Review, 45*(5), 101851. doi:https://doi.org/10.1016/j.pubrev.2019.101851

Schwartz, S., & Ben David, A. (1976). Responsibility and helping in an emergency: Effects of blame, ability and denial of responsibility. *Sociometry*, 406-415.

Schwarz, A. (2008). Covariation-based causal attributions during organizational crises: Suggestions for extending Situational Crisis Communication Theory (SCCT). *International Journal of Strategic Communication, 2*(1), 31-53.

Schwarz, A. (2012). How publics use social media to respond to blame games in crisis communication: The Love Parade tragedy in Duisburg 2010. *Public Relations Review, 38*(3), 430-437. doi:10.1016/j.pubrev.2012.01.009

Seeger, M. W., & Griffin-Padgett, D. R. (2010). From image restoration to renewal: Approaches to understanding postcrisis communication. *The Review of Communication, 10*(2), 127-141. doi:10.1080/1535859090354526

Sellnow, D. D., Johansson, B., Sellnow, T. L., & Lane, D. R. (2019). Toward a global understanding of the effects of the IDEA model for designing instructional risk and crisis messages: A food contamination experiment in Sweden. *Journal of Contingencies and Crisis Management, 27*(2), 102-115. doi:10.1111/1468-5973.12234

Shockley-Zalabak, P. S., Morreale, S., & Hackman, M. (2010). *Building the high-trust organization: Strategies for supporting five key dimensions of trust* (Vol. 7): John Wiley & Sons.

Sohn, Y. J., & Lariscy, R. W. (2014). Understanding reputational crisis: Definition, properties, and consequences. *Journal of Public Relations Research, 26*(1), 23-43. doi:10.1080/1062726X.2013.795865

Stacks, D. W. (2004). Crisis Management: Toward a Multidimension Model of Public Relations. In D. P. Millar & R. L. Heath (Eds.), *Responding to Crisis: A Rhetorical Approach to Crisis Communication* (pp. 37-49). Mahwah, NJ: Lawrence Erlbaum Associates.

Steelman, T. A., & McCaffrey, S. (2013). Best practices in risk and crisis communication: Implications for natural hazards management. *Natural Hazards, 65*(1), 683-705.

Suhr, D. D. (2006). *Exploratory or confirmatory factor analysis?* Paper presented at the SAS Users Group International Conference.

Sullivan, P. (2020, 7 April, 2020). Cyber chiefs warn that Covid-19 remote working 'increasing risk' of breaches. *The Commentator*.

Syed, R. (2019). Enterprise reputation threats on social media: A case of data breach framing. *The Journal of Strategic Information Systems, 28*(3), 257-274. doi:https://doi.org/10.1016/j.jsis.2018.12.001

Takamatsu, M. (2014). The Okinawa Tourism Crisis Management Initiatives. *International Journal of Event Management Research, 8*(1), 19-34.

Tao, W., & Song, B. (2020). The interplay between post-crisis response strategy and pre-crisis corporate associations in the context of CSR crises. *Public Relations Review*, in press. doi:https://doi.org/10.1016/j.pubrev.2020.101883

Uccello, C. (2009). Social interest and social responsibility in contemporary corporate environments. *Journal of Individual Psychology, 65*(4), 412-419.

van Zoonen, W., & van der Meer, T. (2015). The importance of source and credibility perception in times of crisis: crisis communication in a socially mediated era. *Journal of Public Relations Research, 27*(5), 371-388. doi:10.1080/1062726X.2015.1062382

Vogler, D., and Meissner, F. (2020). How users tweet about a cyber attack: An explorative study using machine learning and social network analysis. *Journal of Digital Media & Policy*, 11(2), 195-214.

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.

Weiner, B. (1985). An attributional theory of achievement motivation and emotion. *Psychological review, 92*(4), 548.

Weiner, B. (2006). *Social motivation, justice, and the moral emotions: An attributional approach*: Psychology Press.

Witte, K. (1996). Generating effective risk messages: How scary should your risk communication be? *Communication Yearbook*, 18, 229-254.

Yum, J.-Y., & Jeong, S.-H. (2014). Examining the Public's Responses to Crisis Communication From the Perspective of Three Models of Attribution. *Journal of Business and Technical Communication*, 1050651914560570. doi:10.1177/1050651914560570

Zhou, Z., & Ki, E.-J. (2018). Exploring the role of CSR fit and the length of CSR involvement in routine business and corporate crises settings. *Public Relations Review, 44*(1), 75-83. doi:https://doi.org/10.1016/j.pubrev.2017.11.004

Appendix A: Message Response Provided for the Data Security Crisis

When asked about the situation that you read about, what if your organisation said:

> We value our members and understand the importance of protecting personal information. We have taken measure to investigate and address a data security incident where some of our members private and secure information was accessed. The investigation determined that there was unauthorised access to the database containing all private information about our members. We have reported this incident to law enforcement and continue to support and cooperate in their investigation. We have also begun notifying regulatory authorities. We deeply regret this incident happened. From the start, we moved quickly to contain the incident and conduct a thorough investigation with the assistance of leading security experts. We are working hard to ensure our members have answers to questions about their personal information with a dedicated website and call centre. We are supporting the efforts of law enforcement and working with leading security experts to improve. We are also devoting resources necessary to phase outdated systems and accelerate ongoing security enhancements to our network.

Appendix B: Experimental Design Conditions

Here is a brief summary of the situation you could face…

- **(Bank, Material Blame)** Your bank has suffered a major data breach and your financial details have been compromised. Your bank was made aware six months prior of the possibility for an attack because their IT system's security was flawed and could be susceptible to external threats. Your bank did not update or fix the errors which resulted in the breach of data.
- **(GP, Material Blame)** Your GP surgery has suffered a major data breach and your medical records have been compromised. Your GP surgery was made aware six months prior of the possibility for an attack because their IT system's security was flawed and could be susceptible to external threats. Your GP surgery did not update or fix the errors which resulted in the breach of data.
- **(Bank, No Material Blame)** Your bank has suffered a major data breach and your financial details have been compromised. Your bank had the latest IT system security in place and no prior knowledge of any flaws in their security system. Your bank was unaware of the breach until the data had already been illegally accessed.
- **(GP, No Material Blame)** Your GP surgery has suffered a major data breach and your medical records have been compromised. Your GP surgery had the latest IT system security in place and no prior knowledge of any flaws in their security system. Your GP surgery was unaware of the breach until the data had already been illegally accessed.
- **(Control, Inherent Data Risk)** Institutions like your bank or your GP's surgery both hold private and security information about you and are expected to protect your data. IT systems to protect your data are routinely updated, but there are always potential new threats. When data is illegally accessed these types of institutions sometimes have no knowledge of threats and some have knowledge of potential threats.