Kim, Bokyung; Johnson, Kristine; Park, Sun-Young

Article

Lessons from the five data breaches: Analyzing framed crisis response strategies and crisis severity

Cogent Business & Management

Provided in Cooperation with:
Taylor & Francis Group

Suggested Citation: Kim, Bokyung; Johnson, Kristine; Park, Sun-Young (2017) : Lessons from the five data breaches: Analyzing framed crisis response strategies and crisis severity, Cogent Business & Management, ISSN 2331-1975, Taylor & Francis, Abingdon, Vol. 4, https://doi.org/10.1080/23311975.2017.1354525

Kim et al., *Cogent Business & Management* (2017), 4: 1354525
https://doi.org/10.1080/23311975.2017.1354525

cogent business & management

OPERATIONS, INFORMATION & TECHNOLOGY | RESEARCH ARTICLE

Lessons from the five data breaches: Analyzing framed crisis response strategies and crisis severity

Bokyung Kim[1]*, Kristine Johnson[1] and Sun-Young Park[2]

Abstract: To fill a gap of research that explores cyber crisis management, this study analyzed news stories of the five largest data breaches experienced in 2014 by retailers (i.e. Target, Michaels, Neiman Marcus, Home Depot, and Staples). Corporate crisis communication and its news coverage (n = 64) were evaluated for crisis communication strategies and framed situational factors. Despite companies' use of multiple strategies, newspapers reported their use of advocate strategies more often. Massmediated crisis response strategies were even different among the five companies. Newspapers also reframed crisis severity and crisis controllability. Finally, our findings addressed the key to dealing with the public relations nightmare that would result from a security breach.

Subjects: Organizational Communication; Risk Communication; Marketing; Marketing Communications; Media Communication

Keywords: security breach; data breach; cyber crisis communication; corporate public relations and strategic communication; information management

Received: 14 March 2017
Accepted: 06 July 2017
Published: 25 July 2017

*Corresponding author: Bokyung Kim, Department of Public Relations and Advertising, College of Communication and Creative Arts, Rowan University, Glassboro, NJ, 08028, USA
E-mail: kimb@rowan.edu

Reviewing editor:
Shaofeng Liu, University of Plymouth, UK

Additional information is available at the end of the article

ABOUT THE AUTHOR

Bokyung Kim, PhD, currently teaches at Rowan University as assistant professor of public relations. Kim's background is based primarily in corporate communication research and consulting. Her research agenda centers on corporate transparency, leadership communication, relationship/reputation management, and social media public relations.

Kim received her BA in Mass Communication ('05) from Handong Global University in South Korea, MA in Public Relations ('09) from Michigan State University, and PhD in Strategic Communication ('12) from the University of Missouri. Her first academic posting was at the University of Missouri in 2011 as graduate instructor of record. Kim then moved to her present position at Rowan University in 2012.

Kim's public relations scholarship has been resulted in 21 peer-reviewed conference papers, including a top paper award at the Public Relations Society of America's (PRSA) Health Academy Conference. Her most recent publication appears in the Journalism & Mass Communication Quarterly and Cyberpsychology, Behavior, and Social Networking.

PUBLIC INTEREST STATEMENT

In 2014 hackers were able to access over 85 million consumer accounts from big retails stores. While the effect was severe, little is known of cyber crisis management and media portrayal of hacking and the occurrences. Thus, the researchers sought to evaluate over five dozen newspaper articles about data breaches of the five retail outlets (i.e. Target, Michaels, Neiman Marcus, Home Depot, and Staples); and see if the stories covered in newspapers differed from the public relations strategies directly announced by the affected retail outlets. The newspapers did not match the strategies companies used to deal with data breaches, which made the companies sound like they did not accommodate toward victims and public. Also, news stories described the corporate crises more severe compared to communications issued by the companies. Thus, the authors recommend companies affected by hackers should consider this before announcing how they will respond to a data breach.

1. Introduction

The year 2014 recorded the highest number of consumer accounts breached since 2005, when several companies began tracking the phenomenon when statistics of data breaches were reported and disseminated to the general audience. More than 783 data breach crises occurred in 2014 affecting approximately 85 million consumer accounts across different industries (ITR, 2014). In general, a security breach, or data breach crisis, refers to the loss of consumer information or the fraudulent use of a credit card (Ramakrishna, 2012). While no data are safe from hackers, certain categories of records were targeted disproportionately, and business retailers accounted for about 80% of the individual consumer accounts breached in 2014 (ITR, 2014).

Unlike other data breaches that happened in the US and worldwide, the cases of big retail brands such as Target and Home Depot demonstrate multiple interesting points. First, each of the five data breach crises resulted in millions of compromised consumer accounts, which is regarded as a massive breach crisis: Target (i.e. over 40 million consumer credit card information had been hacked), Home Depot (i.e. more than 56 million consumer credit card data were exposed), Michaels (i.e. 2.6 million accounts), Neiman Marcus (i.e. 1.1 million accounts), and Staples (i.e. 1.2 million accounts). Second, the impact of five data breaches on company performance was severe. For example, Target's stock price fell almost 14% in a couple of months after announcing the data breach crisis on 19 December 2013; and the company saw a 46% year-over-year drop in profits in the fourth quarter of 2013 (Ziobro, 2014). In a similar vein, Home Depot used $62 million in expenses to cover the investigation; the company offered a free credit monitoring service to affected customers, and took other post-crisis management steps (Team, 2014). Third, the five retail companies used immediate and ongoing press releases to deal with data breaches, to inform affected customers about steps to follow, and to woo the general public at large.

For organizations, data breaches present huge challenges: organizations (e.g. banks, financial institutions, health care providers, credit reporting companies, and those who provide consumer information) should comply with legal requirements dictated by the Federal Trade Commission: they should notify all affected and potentially affected customers regarding compromised consumer data, if any. This leads to negative media coverage, which in turn, tarnishes a corporate image and consumer trust (Kelly, 2005). While public relations practitioners cannot necessarily solve all aspects responsible for such security breach crises, they can and often do serve as communication bridges between an organization, its stakeholders and victims, and news media. It includes, but is not limited to, evaluating a given crisis situation to estimate potential reputational and financial damage and employing proper crisis response strategies (CRS).

All in all, the five cases pose several questions about the crisis communication literature. First, the most important lesson from the massive data breaches is to evaluate the situations and see how the retail companies respond to the security breach crises. Is there evidence the five companies had adopted appropriate CRS in a timely manner? With regard to the question, a *Situational Crisis Communication Theory* (SCCT) suggests interconnected situational factors influence an organization's perception of crisis responsibility, which in turn determines the approaches for effective crisis management (Coombs, 2007a).

To be more specific, the SCCT conceptualizes publics' assessment of a crisis by predicting reputational threats posed from organizational factors: Among many situational factors, a crisis type, past crisis history and perceived severity of a crisis have been regarded as important ones in framing and shaping public attribution of crisis responsibility. If a public would solely blame a company facing a crisis considering the three factors, the company should utilize more accommodative strategies such as apology or compensation because of its damaged reputation and greater public expectations toward the company (Coombs, 2004, 2007a, 2007b; Coombs & Holladay, 2002). Thus, this case may illustrate to what degree the five major retail stores' CRS match those suggested by the theory and the situational factors.

Moreover, from the public relations research stream, there is a lack of scholarly research about data breaches in public relations and other communications-related journals. While previous studies focused more on legal issues or technological aspects of data breaches (Kelly, 2005; Ramakrishna, 2012); little is known about how news media as an intermediary public interpret and report data breaches differently from the corporate perspectives in determining the main cause of crisis. Thus, this case may fill the gap by examining various situational factors portrayed by news of the five data breaches and by assessing the manifested type of crisis as to be whether it is viewed as rather severe and predictable.

Therefore, the overarching aim of this research is to identify connections between situational crisis factors and corresponding CRS, as revealed by media coverage and corporate responses. More importantly, this study aims to evaluate whether and how corporate press releases would differ from journalists' framing of news reports depending on the recognition of CRS used by the companies, the negative connotations toward each data breach, the numbers or statistics indicating severity of the crises, and other demonstrated situational factors during the 2014 data breaches.

Consequently, this study employs a content analysis of 64 news stories related to the five security breach crises by analyzing journalists' perceptions in four national online newspapers: *Wall Street Journal* (n = 12); *USA Today* (n = 7); *New York Times* (n = 12); and the *Washington Post* (n = 13). Press releases were obtained from PR Newswire (n = 7) and news releases from official corporate websites (n = 13) were also analyzed in order to directly assess corporate responses. Findings of this study are intended to help public relations scholars and practitioners to attain lessons from previous data breach crisis, and thus, better manage a potential cyber attack crisis.

2. Literature review

2.1. Data breaches and cyber crisis communication research

There appears to be a limited amount scholarly research concerning data breach and cyber crisis management issues in public relations and other related journals. Recent inquires for studies indicate most research stems from publications associated with legal or technological matters. Yet, some may suggest there is some indication of interest in data breach research, as evidenced by the few studies found in communication-related publications.

Previous literature regarding data breaches, or security breach incidents, can be classified into two themes. The first theme addresses issues and key terminologies of data breaches and the impact of data breaches on organizations. This line of research sought to explain the definition of a data breach, why the data breach occurs, and how to reduce the possibility of data breaches.

The ITR defines a data breach as "an incident in which an individual name plus a social security number, driver's license number, medical record or financial record (credit/debit cards included) is potentially put at risk because of exposure (ITR, 2014, p. 2)." More specifically, the most recent data breach reports showed a wide range of industries have faced data breaches: the medical/health care industry (42.5% of incidents), business (33.0%), government/military (11.7%), education (7.3%), and banking/credit/finance (5.5%; ITR, 2014).

In addition, Veltsos (2012) described a data breach as a case when personally identifiable information (PII) is disclosed by a third party; and PII refers to it as "information that can be used to distinguish or trace an individual's identity, such as a full name, address, SSN, date of birth, place of birth, parents' full names, and biometric records (Veltsos, 2012, p. 197)." When PII is used by criminals to create an accurate profile with other Internet data, identity theft would occur, which is a terminology of another cyber crime (Veltsos, 2012).

In such crisis situations, organizations facing data breaches should follow legal ramifications and disclose information to all affected and potentially affected consumers whose data might have been

compromised. These mandatory announcements of data breaches might result in negative media attention, and thus, result in a tarnished corporate image and loss of consumers' trust (Kelly, 2005).

For instance, Cavusoglu and colleagues analyzed newspapers and technological websites (e.g. CNET and ZDNET) to explore the impact of security breaches that occurred between 1996 and 2001 on an organization's performance: announcing security breaches was negatively associated with the market value of the announcing firm (Cavusoglu, Mishra, & Raghunathan, 2004). More specifically, the breached firms lost an average of 2.1% market share within two days of the announcement as well as a $1.65 billion average loss in market capitalization per incident regardless of breach types (Cavusoglu et al., 2004).

As another theme of literature, scholars also recommend taking action by carefully investigating previous data breach reports. For example, in one study, researchers analyzed more than 200 data breach letters and suggested the inclusion of an apology or expression of regret would help create a positive outcome. The authors also indicated the use of visual stimuli—such as noticeable headers—would help readers locate important and relevant information (Jenkins, Anandarajan, & D'Ovidio, 2014).

In another study, Veltsos (2012) examined data breach letters sent by state and federal agencies. It was found most correspondence was formatted using an indirect approach, which indicates information about the breach was not discussed until the end of the letter. According to the author's investigation, data breach information included explanations about the breach, advice on how consumers can deal with the breach and options on how to take accommodative actions. Veltsos suggested a direct approach—meaning the data breach should be addressed at the beginning of the letter—would work better for informing consumers (Veltsos, 2012). Similarly, Kelly emphasized that acting fast is key to dealing with a security breach. Additionally, it was suggested companies should establish effective data security protocols; create a communication template for notifying consumers and potential victims; and constantly update and renew a security program (Kelly, 2005).

Consequently, previous data breach research demonstrates the definitions of a data breach, its negative and significant impact on a company facing a breach crisis, and appropriate templates for informing customers about the data breach. However, research related to data breaches in the context of public relations and crisis communication is very limited. Arguably, this further heightens the need for an investigation of these matters, especially from a crisis response management perspective.

2.2. Situational factors, crisis clusters, and matching crisis response strategies

One of the most rapidly growing bodies of research in public relations is crisis communication. Avery, Lariscy, Kim, and Hocke (2010) quantitatively content analyzed 66 published studies in public relations and communication journals between 1991 and 2009. As a result, the research revealed that Coombs' SCCT (2007a) along with Benoit's image restoration theory is a primary stream of research in crisis management (Avery et al., 2010; Benoit, 1995).

The SCCT provides organizations with ideas to determine how to communicate with their various stakeholders to preserve an organization–public relationship. In general, the theory conceptualizes how organizational reputation is directly and indirectly affected by four situational factors in a crisis situation that deserve our attention: (1) initial crisis responsibility (i.e. stakeholders' perceptions on an organization's personal control of a crisis which is contingent upon crisis types such as a victim, accident, or preventable crisis), (2) crisis history (i.e. presence or absence of a similar crisis in the past), (3) prior reputation (i.e. how an organization treat its publics in a past crisis), and (4) severity of a crisis (i.e. the scale of loss, disaster, injury or destruction caused by a crisis that can increase public evaluation of crisis responsibility; Coombs, 2004, 2007a). Here, crisis responsibility is defined as "the degree to which stakeholders blame the organization for the crisis event" (Coombs, 1998, p. 180).

As a way to repair organizational reputation, crisis communicators should identify a type of given crisis by evaluating the level of crisis responsibility attached to the crisis: (1) a victim cluster which an organization is perceived as the victim of the crisis and attributed the weakest level of crisis responsibility; (2) an accident cluster which the organization is viewed as unintentionally and uncontrollably triggering the crisis and attributed a minimal level of crisis responsibility; and (3) a preventable cluster which the organization is regarded to cause the crisis and attributed the strongest level of crisis responsibility (Coombs, 2007a, 2007b).

Considering the three crisis clusters, crisis communicators can expect different levels of crisis responsibility attributions. In other words, identifying crisis types, crisis history, and crisis severity can restrict the use of CRS to leverage the threat: the higher the level of crisis responsibility an organization has, the more accommodative response strategy it should select (Coombs & Holladay, 1996).

Along the same line, scholars define a comprehensive list of CRS (i.e. attack the accuser, deny, scapegoat, excuse, justification, compensation/corrective action, apology, bolstering, ingratiation, concern/regret; Coombs, 2000; Heath & Coombs, 2006). They also suggest potential CRS that match up with crisis situations to show which strategy works better in a certain crisis situation. For example, organizational reputation benefits when denial strategy options (e.g. denial, shifting the blame, and attack the accuser strategies) are used in response to a victim crisis, and when the diminish response strategies (e.g. excuse and justification) are matched with accidental crises. Additionally, the rebuilding response option (e.g. compensation/corrective action and apology) are useful for accident crises, while bolstering or ingratiation can be used as supplemental strategies with other strategy options (Coombs, 2000, 2007a, 2007b).

The SCCT further locates response strategies along a continuum from defensive to accommodative (Holladay, 2012). In a similar vein, scholars explain an organization facing a conflict situation is likely changing its stance within a continuum from pure advocacy to pure accommodation toward a particular public group (Cameron, Pang, & Jin, 2007; Shin, Cheng, Jin, & Cameron, 2005). From the contingency theory, an organization can take various stances toward different key publics on the continuum, and the dynamics of the process further affect different strategies and tactics an organization may take (Cancel, Cameron, Sallot, & Mitrook, 1997). Here, advocacy means the degree of an organization's strategic position in opposing to the public's viewpoint, whereas accommodation implies the organization's position in favor of its publics (Cameron et al., 2007). Thus, how organizations respond to a crisis varies by what strategy it takes along the continuum from advocacy/defensive options to accommodation in the eyes of key stakeholders. All in all, it is especially important to understand situational factors and perceived crisis types, because those are assumed to determine proper CRS and an organization's strategic position during and after a crisis.

2.3. Mass-mediated strategies and framed crisis responsibility

Recently, there are two themes found in scholarly articles of the SCCT. The first theme is experimentally testing publics' perceptions and evaluations on organizational crisis responses (Coombs & Holladay, 2008, 2009; Jeong, 2009; Kim, Hong, & Cameron, 2014; Kim & Sung, 2014; Sisco, 2012). For example, Coombs and Holladay (2008) compared the three equivalent CRS of apology, compensation, and sympathy and revealed that expressions of sympathy or compensation are just as effective as apology in crises. Similarly, Kim et al. (2014) tested the impact of organizational press releases that voluntarily disclose its crisis on organizational reputation; and suggested using a truth claim (i.e. a claim emphasizing factuality of an official statement) and preemptive disclosure as a proactive crisis communication strategy. Another experimental study of Kim and Sung (2014) found that two-sided messages (i.e. sharing both positive and negative information) in crisis communication were more effective than one-sided messages (i.e. sharing only positive information) in a victim and even a preventable crisis (Kim & Sung, 2014).

Another theme of the SCCT studies has found framing effects of crisis news reports. In a given crisis, publics know about a crisis and gather the crisis-related information from mainstream media,

thus publics' interpretation of a crisis may be influenced by journalists (Bowen & Zheng, 2015; Choi, 2012; Choi & Lin, 2009; Kim & Liu, 2012; Sisco, 2012; Sisco, Collins, & Zoch, 2010). With respect to this concern, crisis information originating from an organization, such as news releases, can also serve as a major information channel for a public. Scholars pointed out general public evaluate a crisis situation based on information from three different sources: information directly generated by an organization experiencing crisis itself, mediated information, and secondhand information from other publics (Coombs & Holladay, 2007; Kim et al., 2014).

In line with this research, Bowen and Zheng (2015) conducted a content analysis of framed crisis responsibility and CRS appearing in news coverage of Toyota's recall crises and showed the corporate official statements employed a full range of CRS; however, those strategies were not equally reported by mass media (Bowen & Zheng, 2015). Another study also quantitatively analyzed and compared traditional and social media response documents of 13 corporate and government organizations to see how they responded to the 2009 flu pandemic (Kim & Liu, 2012). One of the major findings shows that organizations representing corporate interests (e.g. the airline, pharmaceutical, pork production, and food services-related industries) were more frequently adopting denial, diminish, and reinforce response strategies compared to government-related organizations (e.g. the CDC, the Department of Health and Human Services, and the World Health Organization; Kim & Liu, 2012). In a similarly vein, Sisco et al. (2010) examined newspapers to see how they framed crises of American Red Cross; and found that regardless of whether the situation was victim, accidental or preventable, the organization used a diminish strategy which aims to minimize an organization's relationship to a crisis or lessen the perceived severity of the crisis.

In other words, an organization cannot guarantee its official statement will be presented in the crisis news coverage. However, the organization is able to control its official announcement mostly appearing on its press releases. To sum up, crisis information generated by and released from an organization is one of essential crisis tactics; thus, should be considered in our study. Considering the fact that the way mass media frame a crisis can be different from an organization's press releases, we seek to compare the media coverage of communication strategies to what organizations directly release on its official website. Especially, managing corporate communication through CRS is regarded as a strategic way to limit negative media coverage (Ritchie, Dorrell, Miller, & Miller, 2004). Based on literature, the following research question and hypothesis are submitted:

RQ1: Are there differences among the five retailers' news stories (including news releases) when covering CRS?

H1: There are differences between press releases and major newspapers (*The New York Times, Wall Street Journal, USA Today*, and *The Washington Post*) in reporting CRS.

As we pointed out, few studies have examined data breaches or any other security breach crises in the context of the SCCT and crisis communication. Most notably, little is known of what type of crisis the five data breaches could fall under. In addition, we would like to examine what strategies are considered as appropriate in terms of the framed crisis category. Noteworthy, Ramakrishna (2012) argues that recent data breaches are believed to be human errors (i.e. crises caused by careless employees in protecting consumer information, outdated security programs, and a lack of proper employee training and administrative security policies). In addition, Jenkins et al. (2014) suggested employing an apology and expression of regret in dealing with data breaches in order to create a positive outcome. In this study, based on the previous findings, we will determine the perceived type of the five data breach crises via assessing situational factors (i.e. controllability of a crisis and crisis history) and another importance modifying situational factor (i.e. crisis severity) through news stories and corporate press releases. To summarize the previous discussions, these are research questions that will be analyzed:

RQ2: Are there differences between major newspapers and press releases in framing the type of data breach crises?

RQ3: Are there differences between major newspapers and press releases when reporting severity of the five data breaches?

RQ4: Are there differences among the five retailers' news stories (including press releases) when reporting crisis severity?

3. Method

3.1. Study design

To address research questions and hypotheses, we conducted a quantitative content analysis to examine news coverage concerning the five major data breaches of retail companies happened in 2014 having more than one million victims in the US (Target, Michaels, Neiman Marcus, Home Depot, and Staples; ITR, 2014).

To retrieve news stories, we used the ProQuest database given it includes the major US newspapers. We then selected the top four newspapers (i.e. *New York Times*, *The Washington Post*, *USA Today*, and *Wall Street Journal*) in terms of their national circulation and impact.

We focused on the data breaches that occurred from 20 December 2013 (i.e. we included this timeline as the Target case broke on 20 December 2013) through 31 December 2014, and searched the ProQuest for three keywords that appeared in both the title and story: "data breach," "identity theft," and "cyber threat." We retrieved 115 stories from the four media outlets. Our research protocol then excluded duplicates and unrelated items such as opportunistic advertising by companies using the data breach crisis to promote their services and products. Eventually, we obtained 44 news articles in our media sample.

PR Newswire ($n = 7$) and press releases ($n = 13$) were obtained from the breached firms' official websites and were chosen as alternative databases to supplement the news articles because they included full coverage of corporate responses and strategies. This study identified a total of 65 news stories including 12 (18.75% of the entire sample) from *New York Times*, 7 (10.94%) from PR Newswire, 7 (10.94%) from *USA Today*, 13 (20.31%) from *Washington Post*, 12 (18.75%) from *Wall Street Journal*, and 13 (20.31%) from press releases; and including 12 (18.75%) news stories from *Target*, 7 (10.94%) from *Michaels*, 5 (7.81%) from *Neiman Marcus*, 32 (50%) from *Home Depot*, and 8 (12.5%) from *Staples*. We examined the full text content of one press release and one newspaper article as the unit of analysis (see Table 1).

Table 1. Data summary: number of news stories per publication and timeline

Timeline	NYT	PRN	UT	WP	WSJ	PR	Total
December, 2013	1	1	0	0	0	7	9
January, 2014	0	0	0	3	2	2	7
April, 2014	1	0	0	1	0	1	3
June, 2014	0	0	0	0	0	1	1
September, 2014	5	5	3	5	5	0	23
October, 2014	1	0	2	2	1	0	6
November, 2014	3	1	0	1	3	1	9
December, 2014	1	0	2	1	1	1	6
Total	12	7	7	13	12	13	64

3.2. Coding categories

For both press releases and newspapers, the categories of analysis included the posted/issued date, the source of news stories, the company names, types of each public mentioned in the stories (inclusive of title), situational factors (i.e. crisis history, controllability of a crisis, and crisis severity), and CRS.

3.2.1. Types of publics/organizations mentioned in the news

The presence or absence of each type of publics was coded: (1) hackers (criminals, cyber criminals, thieves, etc.); (2) victims (credit card or bank account holders whose information were compromised); (3) general public (customers, people, and shareholders); 4) other companies having similar data breach crises; (5) legal parties (e.g. LLP's offering to service customers whose data were compromised); and (6) government (e.g. US District Judge, FBI; US Secret Service, NY Attorney General, Police).

3.2.2. Crisis response strategies

This research identified the response strategies via answering the questions (1 = yes and 0 = no) according to their operationalized definitions. CRS used by each company to respond to lay public and victims were coded. Based on the initial typology and the modified typology of CRS (Coombs, 2000; Holladay, 2012; Pace, Fediuk, & Botero, 2010), the nine strategies were measured: (1) attack the accuser (i.e. a company threatened to sue journalists/customers who claim a crisis occurred); (2) denial (e.g. *Target spokesman confirmed it has no indication that debit card personal identification number were impacted*), (3) scapegoat (e.g. *hackers were responsible for causing this massive data breach at Staples*); (4) excuse (i.e. minimizing its responsibility by claiming inability to control a crisis; *Michaels Stores said it may have been the victim of an attack on its data security and it happened as part of the operation of any organization*); (5) justification (i.e. explaining crisis damage were minor; *the retailer said the breach affected customers who shopped in stores, but not online. Only email addresses were compromised*); (6) ingratiation (i.e. thanking stakeholders for their help and reminded them of the organization's past great performances); (7) compensation (i.e. correcting the source of the problem and addressing the victim's needs; *Home Depot said it would offer free identify protection and credit monitoring services to any customer who had used a credit or debit card at any of its affected stores*); (8) regret (i.e. expressing remorse about having caused crisis to stakeholders; *Neiman Marcus CEO said,* "We deeply regret the data breach."); and (9) apology (i.e. taking full responsibility the data breaches or releasing official apologies to publics).

3.2.3. Crisis severity

Crisis severity was coded via answering the questions (1 = yes and 0 = no) of whether the news story mentioned any negative connotations (e.g. "the largest hack ever," "one of the major data breach scandals in the US," or "a severe security breach"); and whether the particular article included any related statistics indicating severe damage of a data breach such as a number of victims and economic cost to the breached firms.

3.2.4. Crisis history

Crisis history was coded as another significant situational factor determining the perceived type of crisis, based on whether a given news story mentioned a past crisis history of the breached retailers.

3.2.5. Crisis controllability

Crisis controllability/intentionality to allow a data breach was coded via answering to a question (1 = yes and 0 = no) of whether the story suggests that the breached firm has the ability to alleviate the problem (e.g. pre-existing weaknesses in data protection and policy, outdated security programs, etc.).

3.3. Coding procedure and inter-coder reliability

Two coders were trained to a pilot-tested codebook. Each coded a randomly selected subsample 10 (15.38%) of the data to get an inter-coder reliability of .82 (Krippendorf's *R*) for negative

connotations, .84 for crisis severity (i.e. mentioning significant numbers and statistics), .76 for crisis history; .76 for crisis type (i.e. controllability of a crisis); and .79 for response strategies, indicating that the agreement between the coders was acceptable. Two coders then coded the rest of the news articles and press releases independently.

4. Results

RQ1 addressed CRS used by the five retailers (i.e. to respond to affected consumers and lay public) that appeared in news coverage and their press releases. As shown in Table 2, there was a significant difference in reporting such CRS as denial (χ^2 (4) = 9.92, $p < .05$), regret (χ^2 (4) = 11.71, $p < .05$), and apology (χ^2 (4) = 15.75, $p < .01$) between the five retailers' data breaches. That is, news stories about Neiman Marcus (20% of its news stories) and Michaels (28.6% of its news stories) reported the retailers' denial strategy more often. On the contrary, news stories of Home Depot (84.4% of its news outlets) and Target (75% of its news stories) did not recognize the two companies' expressions of regret to its publics. In a similar vein, 40% of all Neiman Marcus' news stories mentioned the corporate official apology statement. However, only 12.5% of news stories of Home Depot and 8.3% of Target's news coverage acknowledged the two breached firms' apology statements (see Table 2).

Table 2. χ^2 tests for crisis response strategies by five retailers

CRS	Target (*n* = 12)	Michaels (*n* = 7)	Neiman marcus (*n* = 5)	Home depot (*n* = 32)	Staples (*n* = 8)	χ^2	df	Sig.
Denial								
Yes	2 (16.7%)	2 (28.6%)	1 (20%)	0 (0%)	0 (0%)	9.92	4	$p < .05$
No	10 (83.3%)	5 (71.4%)	4 (80%)	32 (100%)	8 (100%)			
Scapegoat								
Yes	2 (16.7%)	2 (28.6%)	1 (20%)	13 (40.6%)	4 (50%)	3.65	4	*n.s.*
No	10 (83.3%)	5 (71.4%)	4 (80%)	19 (59.4%)	4 (50%)			
Excuse								
Yes	2 (16.7%)	2 (28.6%)	1 (20%)	9 (28.1%)	5 (62.5%)	5.37	4	*n.s.*
No	10 (83.3%)	5 (71.4%)	4 (80%)	23 (71.9%)	3 (37.5%)			
Justification								
Yes	5 (41.7%)	5 (71.4%)	3 (60%)	13 (40.6%)	5 (62.5%)	3.39	4	*n.s.*
No	7 (58.3%)	2 (28.6%)	2 (40%)	19 (59.4%)	3 (37.5%)			
Ingratiation								
Yes	3 (25%)	4 (57.1%)	2 (40%)	17 (53.1%)	1 (12.5%)	3.86	4	*n.s.*
No	9 (75%)	3 (42.9%)	3 (60%)	15 (46.9%)	7 (87.5%)			
Compensation								
Yes	10 (83.3%)	4 (57.1%)	4 (80%)	17 (53.1%)	6 (75%)	4.77	4	*n.s.*
No	2 (16.7%)	3 (42.9%)	1 (20%)	15 (46.9%)	2 (25%)			
Regret								
Yes	3 (25%)	4 (57.1%)	3 (60%)	5 (15.6%)	0 (0%)	11.71	4	$p < .05$
No	9 (75%)	3 (42.9%)	2 (40%)	27 (84.4%)	8 (100%)			
Apology								
Yes	1 (8.3%)	0 (0%)	2 (40%)	4 (12.5%)	0 (0%)	15.75	4	$p < .01$
No	11 (91.7%)	7 (100%)	3 (60%)	28 (87.5%)	8 (100%)			

Notes: χ^2: The chi-square (χ^2) statistic is used to investigate whether distribution of categorical variables differ from one another. In other words, the above χ^2 statistic compares counts of crisis response strategies used by five companies and analyzes whether there is a statistically significant relationship between the five companies and their crisis response strategies. That is, if the *p*-value (see the column, Sig.) is less than 0.5, it indicates that there is a statistically significant difference in using each crisis response strategy among the five companies. Here, "*n.s.*" refers to "not significant."

Table 3. χ^2 results of crisis response strategies by two media outlets

Crisis response strategies	Newspapers (*n* =44)	Press releases (*n* = 20)	χ^2	df	Sig.
Denial					
Yes	0 (0%)	5 (25%)	11.93	1	$p < .001$
No	44 (100%)	15 (75%)			
Scapegoat					
Yes	20 (45.5%)	2 (10%)	7.66	1	$p < .01$
No	24 (54.5%)	18 (90%)			
Excuse					
Yes	19 (43.2%)	0 (0%)	12.28	1	$p < .001$
No	25 (56.8%)	20 (100%)			
Justification					
Yes	22 (50%)	9 (45%)	.14	1	*n.s.*
No	22 (50%)	11 (55%)			
Ingratiation					
Yes	12 (27.3%)	15 (75%)	10.78	1	$p < .01$
No	32 (72.7%)	5 (25%)			
Compensation					
Yes	27 (61.4%)	14 (70%)	.45	1	*n.s.*
No	17 (38.6%)	6 (30%)			
Regret					
Yes	7 (15.9%)	8 (40%)	4.45	1	$p < .05$
No	37 (84.1%)	12 (60%)			
Apology					
Yes	0 (0%)	7 (35%)	3.57	1	$p = .056$
No	44 (100%)	13 (65%)			

Notes: χ^2: The chi-square (χ^2) statistic is used to compare counts of crisis response strategies reported through online newspapers and corporate press releases and analyzes whether there is a statistically significant relationship between the two sources and their crisis response strategies reports. That is, if the *p*-value (see the column, Sig.) is less than 0.5, it indicates that there is a statistically significant difference in reporting each crisis response strategy between the newspapers and corporate press releases. Here, "*n.s.*" refers to "not significant."

The first hypothesis tried to detect the possible difference between major newspapers and retailers' press releases in reporting CRS. In χ^2 results, newspapers used such strategies as scapegoat (χ^2 (1) = 7.66, $p < .01$) and excuse (χ^2 (1) = 12.28, $p < .001$) strategies significantly more often than the retailers' news releases. Conversely, the five retailers used the following strategies significantly more often than newspapers: denial (χ^2 (1) = 11.93, $p < .001$), ingratiation (χ^2 (1) = 10.78, $p < .01$), and regret (χ^2 (1) = 4.45, $p < .05$). Additionally, the difference between newspapers and press releases in reporting an apology was close to statistical significance: corporate press releases used apology more often compared to newspapers (see Table 3).

RQ2 addressed the possible difference between newspaper and corporate press releases in framing the crisis type. As shown in Table 4, there was no significant difference in how newspapers and corporate news releases report controllability of the crises, χ^2 (1) = .95, $p = .33$. Noteworthy, the difference between the two media outlets in reporting past crisis history of retailers was close to statistical significance (χ^2 (1) = 3.58, $p = .056$): newspapers ($n = 7$, 15.9%) mentioned past crisis of the breached firms more often than corporate press releases ($n = 0$. 0%).

Table 4. χ^2 results of framed crisis type by two media outlets

	Framed controllability of a data breach		Total
	No	Yes	
Major newspapers	30 (68.2%)	14 (31.8%)	44 (100%)
Press releases	16 (80.0%)	4 (15.0%)	20 (100%)
Total	46	18	64
χ^2 (1) = .95, *n.s.*			
	Mention any past crisis of the retailers, if any		Total
	NO	Yes	
Major newspapers	37 (84.1%)	7 (15.9%)	44 (100%)
Press releases	20 (100 %)	0 (.0%)	20 (100%)
Total	57	7	64
χ^2 (1) = 3.58, p = .056			

Notes: χ^2: The chi-square (χ^2) statistic is used to compare counts of framed crisis controllability and crisis history reported through online newspapers and corporate press releases and analyzes whether there is a statistically significant relationship between the two sources and their framed crisis types. That is, if the p-value is less than 0.5, it indicates that there is a statistically significant difference in reporting and framing crisis types between the newspapers and corporate press releases. Here, "*n.s.*" refers to "not significant."

Table 5. χ^2 results of framed crisis severity by two media outlets

	Negative connotations in reporting damage of a data breach		**Total**
	No	**Yes**	
Major newspapers	25 (56.8%)	19 (43.2%)	44 (100%)
Press releases	17 (85.0%)	3 (15.0%)	20 (100%)
Total	42	22	64
χ^2 (1) = 4.84, p < .05			

RQ3 attempted to explore whether there are differences in how newspapers and press releases report the severity of the five data breaches. As shown in Table 5, major newspapers (n = 19, 43.2%) used many more negative connotations of the severity of data breaches than retailers' press release (n = 3, 15%).

Finally, RQ4 examined whether and how news stories (including press releases) framed severity of and the predictability of the five retailers' data breaches differently. There were no significant differences in reporting the severity among the five retailers' news stores in terms of using negative connotations, χ^2 (4) = 7.39, p = .11, and mentioning statistics regarding the damage of an issue, χ^2 (4) = 4.91, p = .29. With regard to framing the crisis type, the crisis controllability of the five retailers

Table 6. χ^2 results of framed crisis type by five retailers

	Framed controllability of a data breach		**Total**
	No	**Yes**	
Target	12 (26.1%)	0 (0.0%)	12 (100%)
Michaels	7 (15.2%)	0 (0.0%)	7 (100%)
Neiman Marcus	5 (10.9%)	0 (0.0%)	5 (100%)
Home depot	15 (32.6%)	17 (94.4%)	32 (100%)
Staples	7 (15.2%)	1 (5.6%)	8 (100%)
Total	46	18	64
χ^2 (4) = 20.25, p < .001			

were significantly differently addressed in news stories, χ^2 (4) = 20.25, $p < .001$ (see Table 6). On the other hand, in terms of reporting the past crisis history, the significant difference among the five retailers was not observed, χ^2 (4) = 3.80, $p = .43$.

5. Discussion

The primary goal of this research was to examine the manner in which prestige newspapers and corporate news releases reported the five largest data breach crises from 20 December 2013 through 31 December 2014. Using a quantitative content analysis of 64 news stories, media coverage messages and corporate communication messages were compared. Specifically, this study sought to explore whether and how journalists were different from the breached firms in their recognition of CRS used by the retailers, understanding of crisis situations and severity, and reporting past crisis history of the five companies.

The first hypothesis in this study asked which response strategies the five retailers employed and published in major news outlets and their official websites. While the five retailers used a full range of response strategies including denial, ingratiation, and regret, news media outlets assessed that the breached firms chose more advocate strategies such as scapegoat or excuse. It is consistent with previous findings (Bowen & Zheng, 2015; Nijkrake, Gosselt, & Gutteling, 2015) in that the news media reframed corporate communication strategies and reported different communication messages than the organizations in crisis. In other words, journalists' acknowledgment of CRS can be dissimilar to what organizations actually use.

Most notably, the strategic options the breached firms adopted were somewhat different among the five retailers. To illustrate, our results show that news stories about Neiman Marcus and Michaels frequently reported their adoption of denial as more defensive strategy. For example, the two companies constantly used such denial strategy in their news releases as follows: "there is NO indication that our customer credit cards have been used fraudulently," "receiving an email from us is absolutely not an indication that there has been, or will be, fraud on their card," or "the investigation found no malware or suspicious activity related to the payment systems at our stores." Considering the relatively small numbers of compromised records of the two companies compared to other severe breaches (e.g. 2.6 million affected accounts of Michaels and 1.1 million of Neiman Marcus), this strategy could be useful in dealing with the particular two cases.

It also aligned with previous findings regarding the most frequently used response strategies (Kim, Avery, & Lariscy, 2009). Scholars have argued regarding the issue that whether denial is helpful only in a victim crisis, when an organization is not viewed as responsible for the crisis (Heath & Coombs, 2006). Kim and colleagues also emphasized that organizations in their sample tend to use denial "without considering contextual moderators of when it should be used" (Kim et al., 2009, p. 448). According to a study of van der Meer (2014) however, denial could be effective in certain situations, if public would adopt an organizations' crisis-denial frame as time goes by.

On the contrary, news stories of Home Depot (i.e. record: 56 million) and Target (i.e. record: 40 million), which are the two largest security breach incidents in 2014, did not mention their use of regret and apology. To sum up, news stories about less severe data breach crises reported more defensive CRS used by the companies such as denial, while news articles of the most severe crises (i.e. Target or Home Depot) did not mention their use of accommodative strategies (i.e. regret and apology). This finding can also be a red flag of cyber crisis management; especially because it is assumed that apology and regret are effective strategies in security breaches (Jenkins et al., 2014).

This study then detected the dissimilar approaches by which mass media and the breached companies understand and frame the crises. In regard to the research questions examining framed controllability of the five data breaches, there were no significant differences between major newspaper and corporate communication messages. However, the crisis controllability was differently addressed among the five retailers. Aligned with findings above, the case of Home Depot was

portrayed as more predictable and controllable in causing its data breach compared to other breach crises, whereas the three cases experiencing relatively less severe attack (Neiman Marcus, Michaels, and Staples) were viewed as less controllable. In other words, the breach crisis of Home Depot could pose a greater reputational threat to the retailer than other cases, as mainstream media portrayed that crisis as controllable (i.e. categorized as an intentional crisis cluster).

Furthermore, the major newspapers framed damage of a crisis more severe in which the event was described, compared to communications issued by an organization. In other words, newspapers tended to emphasize the massive damage of each data breach crisis, through citing victim experiences and magnifying the negative outcomes (e.g. the media mentioned negative connotations such as "the largest data breach in the US history" and "the massive hack ever").

In short, in spite of crisis communication messages, news media seem to introduce their own stories in ways that demonstrate damage of incident and which party can be held responsible. If an organization's crisis situation is reframed by the news media as the way our data suggest, the reframed crisis severity and crisis controllability are a call-to-action for public relations professionals to deal with a cyber attack crisis. Given that crisis responsibility attribution to a company can be modified by crisis severity perceptions, the breached firm is expected to not only analyze its reality, but also monitor corporate crisis communication and its news coverage.

Considering both literature and our findings, one might wonder how crisis managers should deal with a data breach crisis concerning its unique crisis context. The most important practical implication is that crisis communicators should evaluate a cyber crisis situation in terms of how an organization's initial response strategies are adopted and published in news media platform. If newspapers frame a breached firm using more defensive and advocate response strategies, the organization should adjust and correctly inform its communication messages to news media, which in turn, flow to general public. Also, concerning the reframed crisis type and crisis severity evidenced in news stories, public relations practitioners should keep an eye on news outlets, especially if they frame security breach cases as more severe and controllable as our data suggest.

Similar to other content analyses, this study was limited in that we employed the quantitative content analysis of news articles and corporate news releases. Given the rising popularity of social media, future research may contain other digital media such as weblogs, social media sites, and other online postings of more involved publics (e.g. affected consumers) to reflect much variation of other public groups and their evaluations on the corporate CRS and the situation of a data breach. Additionally, this study only retrieved 20 press releases directly from retailers; less than the 44 news stories retrieved from newspapers. The difference in the amount of each story type could influence the statistical results. Third limitation concerns the industry type of data breaches, which is used for this study. This research only included business retailers concerning the fact that they accounted for 79.7% of breached records in 2014 (ITR, 2014). We recommend continued study in other data breach crisis context using such other industry sectors as health care industry, government, and/or banking/credit/finance. Along the same line, based on our findings future research may conduct experimental studies to investigate how stakeholders perceive a data breach crisis, how they attribute crisis responsibility for the cyber attack, and which response strategies gain more public support.

6. Conclusion

In conclusion, the result of this analysis offers great promise to crisis communication scholars and practitioners seeking to better understand the nature of unexpected cyber attack. There is significant potential for monitoring mass-mediated crisis communication strategies and evaluating framed crisis situations which are constructed by news outlets, if there are dissimilar approaches as the way our data suggest.

Funding
The authors received no direct funding for this research.

Author details
Bokyung Kim[1]
E-mail: kimb@rowan.edu
Kristine Johnson[1]
E-mail: johnsonkr@rowan.edu
Sun-Young Park[2]
E-mail: SunYoung.Park@umb.edu
[1] Department of Public Relations and Advertising, College of Communication and Creative Arts, Rowan University, Glassboro, NJ, 08028, USA.
[2] Department of Communication, College of Liberal Arts, University of Massachusetts, Boston, MA, USA.

Citation information
Cite this article as: Lessons from the five data breaches: Analyzing framed crisis response strategies and crisis severity, Bokyung Kim, Kristine Johnson & Sun-Young Park, *Cogent Business & Management* (2017), 4: 1354525.

References

Avery, E. J., Lariscy, R. W., Kim, S., & Hocke, T. (2010). A quantitative review of crisis communication research in public relations from 1991 to 2009. *Public Relations Review, 36*, 190–192. https://doi.org/10.1016/j.pubrev.2010.01.001

Benoit, W. L. (1995). *Accounts, excuses, and apologies: A theory of image restoration strategies*. Albany: State University of New York.

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

Cameron, G. T., Pang, A., & Jin, Y. (2007). Contingency theory: Strategic management of conflict in public relations. In T. Hansen-Horn, & B. Neff (Eds.), *Public relations: From theory to practice* (pp. 134–157). Boston, MA: Pearson Allyn & Bacon.

Cancel, A. E., Cameron, G. T., Sallot, L. M., & Mitrook, M. A. (1997). It depends: A contingency theory of accommodation in public relations. *Journal of Public Relations Research, 9*, 31–63. https://doi.org/10.1207/s1532754xjprr0901_02

Cavusoglu, H., Mishra, B., & Raghunathan, S. (2004). The effect of internet security breach announcements on market value: Capital market reactions for breached firms and internet security developers. *International Journal of Electronic Commerce, 9*, 69–104.

Choi, J. (2012). A content analysis of BP's press releases dealing with crisis. *Public Relations Review, 38*, 422–429. https://doi.org/10.1016/j.pubrev.2012.03.003

Choi, Y., & Lin, Y.-H. (2009). Consumer responses to Mattel product recalls posted on online bulletin boards: Exploring two types of emotion. *Journal of Public Relations Research, 21*, 198–207. https://doi.org/10.1080/10627260802557506

Coombs, W. T. (1998). An analytic framework for crisis situations: Better responses from a better understanding of the situation. *Journal of Public Relations Research, 10*, 177–191. https://doi.org/10.1207/s1532754xjprr1003_02

Coombs, W. T. (2000). Designing post-crisis messages: Lessons for crisis response strategies. *Review of Business, 21*, 37–41.

Coombs, W. T. (2004). Impact of past crises on current crisis communication: Insights from situational crisis communication theory. *Journal of Business Communication, 41*, 265–289.

Coombs, W. T. (2007a). Protecting organization reputations during a crisis: The development and application of situational crisis communication theory. *Corporate Reputation Review, 10*, 163–176. https://doi.org/10.1057/palgrave.crr.1550049

Coombs, W. T. (2007b). *Ongoing crisis communication: Planning, managing, and responding* (2nd ed.). Thousand Oaks, CA: Sage.

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*, 279–295. https://doi.org/10.1207/s1532754xjprr0804_04

Coombs, W. T., & Holladay, S. J. (2002). Helping crisis managers protect reputational assets. *Management Communication Quarterly, 16*, 165–186.

Coombs, W. T., & Holladay, S. J. (2007). The negative communication dynamic: Exploring the impact of stakeholder affect on behavioral intentions. *Journal of Communication Management, 11*, 300–312.

Coombs, W. T., & Holladay, S. J. (2008). Comparing apology to equivalent crisis response strategies: Clarifying apology's role and value in crisis communication. *Public Relations Review, 34*, 252–257. https://doi.org/10.1016/j.pubrev.2008.04.001

Coombs, W. T., & Holladay, S. J. (2009). Further explorations of post-crisis communication: Effects of media and response strategies on perceptions and intentions. *Public Relations Review, 35*(1), 1–6. https://doi.org/10.1016/j.pubrev.2008.09.011

Heath, R. L., & Coombs, W. T. (2006). *Today's public relations: An introduction*. Thousand Oaks, CA: Sage.

Holladay, S. J. (2012). Are they practicing what we are preaching? An investigation of crisis communication strategies in the media coverage of chemicalaccidents. In W. T. Coombs, & S. Holladay (Eds.), *The handbook of crisis communication* (pp. 159–180). MA: Wiley Blackwell.

ITR. (2014). *Identity theft resource center breach reports*. Retrieved from https://www.idtheftcenter.org/images/breach/DataBreachReports_2014.pdf

Jenkins, A., Anandarajan, M., & D'Ovidio, R. (2014). All that glitters is not gold: The role of impression management in data breach notification. *Western Journal of Communication, 78*, 337–357. https://doi.org/10.1080/10570314.2013.866686

Jeong, S. H. (2009). Public's responses to an oil spill accident: A test of the attribution theory and situational crisis communication theory. *Public Relations Review, 35*, 307–309. https://doi.org/10.1016/j.pubrev.2009.03.010

Kelly, C. (2005). Data security: A new concern for PR practitioners. *Public Relations Quarterly, 50*, 25–26.

Kim, S., Avery, E. J., & Lariscy, R. W. (2009). Are crisis communicators practicing what we preach? An evaluation of crisis response strategy analyzed in public relations research from 1991 to 2009. *Public Relations Review, 35*, 446–448. https://doi.org/10.1016/j.pubrev.2009.08.002

Kim, S., & Liu, B. F. (2012). Are all crises opportunities? A comparison of how corporate and government organizations responded to the 2009 Flu Pandemic. *Journal of Public Relations Research, 24*, 69–85. https://doi.org/10.1080/1062726X.2012.626136

Kim, B., Hong, S., & Cameron, G. T. (2014). What corporations say matters more than what they say they do? A test of a truth claim and transparency in press releases on corporate websites and facebook pages. *Journalism & Mass Communication Quarterly, 91*, 811–829. https://doi.org/10.1177/1077699014550087

Nijkrake, J., Gosselt, J. F., & Gutteling, J. M. (2015). Competing frames and tone in corporate communication versus media coverage during a crisis. *Public Relations Review, 41*, 80–88. https://doi.org/10.1016/j.pubrev.2014.10.010

Pace, K. M., Fediuk, T. A., & Botero, I. C. (2010). The acceptance of responsibility and expressions of regret in organizational apologies after a transgression. *Corporate*

Communications: An International Journal, 15, 410–427. https://doi.org/10.1108/13563281011085510

Ramakrishna, A. (2012). An exploratory analysis of data breaches from 2005-2011: Trends and insights. *Journal of Information Privacy & Security, 8*, 33–56.

Ritchie, B. W., Dorrell, H., Miller, D., & Miller, G. A. (2004). Crisis communication and recovery for the tourism industry. *Journal of Travel & Tourism Marketing, 15*, 199–216. https://doi.org/10.1300/J073v15n02_11

Shin, J., Cheng, I., Jin, Y., & Cameron, G. T. (2005). Going head to head: Content analysis of high profile conflicts as played out in the press. *Public Relations Review, 31*, 399–406.

Sisco, H. F. (2012). Nonprofit in crisis: An examination of the applicability of situational crisis communication theory. *Journal of Public Relations Research, 24*(1), 1–17. https://doi.org/10.1080/1062726X.2011.582207

Sisco, H. F., Collins, E. L., & Zoch, L. M. (2010). Through the looking glass: A decade of red cross crisis response and situational crisis communication theory. *Public Relations Review, 36*, 21–27. https://doi.org/10.1016/j.pubrev.2009.08.018

Team, T. (2014). *Home depot: Could the impact of the data breach be significant?* Retrieved from https://www.forbes.com/sites/greatspeculations/2014/09/24/home-depot-could-the-impact-of-the-data-breach-be-significant/

van der Meer, T. G. L. A. (2014). Organizational crisis-denial strategy: The effect of denial on public framing. *Public Relations Review, 40*, 537–539. https://doi.org/10.1016/j.pubrev.2014.02.005

van der Meer, T. G. L. A., Verhoeven, P., Beentjes, H., & Vliegenthart, R. (2014). When frames align: The interplay between PR, news media, and the public in times of crisis. *Public Relations Review, 40*, 751–761. https://doi.org/10.1016/j.pubrev.2014.07.008

Veltsos, J. R. (2012). An analysis of data breach notifications as negative news. *Business Communication Quarterly, 75*, 192–207. https://doi.org/10.1177/1080569912443081

Ziobro, P. (2014). *Target earnings slide 46% after data breach*. Retrieved from https://www.wsj.com/articles/SB10001424052702304255604579406694182132568

Cogent Business & Management **(ISSN: 2331-1975) is published by Cogent OA, part of Taylor & Francis Group.**