A STUDY OF ORGANIZATIONAL RESPONSES TO MAJOR DATA BREACHES IN THE RETAIL & HEALTHCARE INDUSTRIES

Charles A. Lubbers, University of South Dakota

Allison McNamara, University of South Dakota

Yuxiao Lu, University of South Dakota,

Tanner Sifferath, University of South Dakota

ABSTRACT

Coombs' crisis communication response strategies were used to conduct a content analysis of corporate responses to data breaches in the U.S. healthcare and business industries. Twenty of the largest incidents of a data breach during 2014 were studied. The organization's responses from the ten largest breaches during 2014 in U.S. healthcare and business/retail industry categories were studied to learn common practices when responding to data breaches. A content analysis instrument was developed that incorporated categories of responses identified by Coombs and others. Two coders reviewed the organization's response and recorded the appropriate information on the coding sheet. Efforts were taken to ensure inter-coder reliability. This exploratory research discovered that four of Coombs' response strategies were regularly employed across the responses studied and that content from eight categories identified during the coding was located in at least half of the corporate responses. There is a great opportunity for further research, as little research has been conducted for such a large and important field.

Keywords: data breach, response strategies, crisis communication

INTRODUCTION

"It's the phone call everyone dreads making. The one to your credit card company, asking why your MasterCard didn't work at Trader Joe's. You listen to awful elevator music for thirty minutes, before you're granted the privilege of talking to some grumpy bank employee. When you finally are allowed to speak to a human being, she asks if you really did buy five thousand plastic pink flamingo decorations on November 15th, 2013. Of course you say, 'No, I didn't do that.' That's when you find out someone stole your identity. That's when you find out what a data breach is; that it doesn't matter how careful you are, or that your bank is careful too. At any rate, you definitely need to find out if you can be reimbursed for those five thousand flamingos" (Dwyer, 2014, p. 6).

Dwyer's (2014) scenario highlights a growing problem, identity theft from stolen information. How that information secured, however, determines whether you have been the victim of a data breach as a result of an organization's failure to secure your private information. The Identify Theft Resource Center (ITRC) defines a breach "as an event in which an individual's name plus

Social Security Number (SSN), driver's license number, medical record, or a financial record/credit/debit card is potentially put at risk – either in electronic or paper format" (2013). Unfortunately, data breaches have become more common.

Frei (2014) notes that "the frequency with which data breaches occur and the number of records that are lost in those breaches has increased considerably within the past decade. Figure 1 depicts the top ten largest data breaches of the past decade as of January 2014. Half of these breaches occurred in 2013 alone, with a total of 512 million records lost that year" (4). The growth in 2013 is significant, since Kumar (2014) notes that the number of security breaches rose 62% in 2013.

Figure 1. Top 10 Data Breaches of Past Decade – as of January 2014

1	Oct 2013	Adobe Systems, Inc	152 M	US
2	Mar 2012	Shanghai Roadway D&B Marketing Services Co. Ltd	150 M	CN
3	Jun 2013	Multiple South Korean businesses	140M	KR
4	Jan 2009	Heartland Payment Systems	130 M	US
5	Dec 2013	Target Brands, Inc.	110 M	US
6	Jan 2007	TJX Companies Inc.	94 M	US
7	Apr 2011	Sony Corporation	77 M	JP
8	Mar 2013	IRS agents allegedly seized 60M records of 10M people during raid	60M	?
9	Aug 2008	Government agencies, state firms, telecom companies	50M	US
10	Apr 2013	LivingSocial Inc.	50M	US

Top 10 Largest Data Breaches with Number of Lost Records in Millions [Source: DataLossDB]

Data breaches affect a wide variety of organizations. The ITRC analysis of breaches in the US during 2013 and 2014 led to Figure 2. Clearly the business sector suffered the most breaches, with approximately one-third of the breaches and around 80% percent of the records in both years. The category with the largest percentages of the breaches was the medical/healthcare industry, with nearly 43% of the breaches both years, but those breaches accounted for just under 10% of the records.

Figure 2. US Data Breaches in 2013 and 2014 by Industry Category

Banking, Credit, Financial	3.7%	1.4%	5.5%	1.4%
Business	33.9%	81.7%	33.0%	79.7%
Educational	9.0%	5.6%	7.3%	1.5%
Government, Military	10.2%	3.3%	11.7%	7.8%
Medical, Healthcare	43.1%	8.1%	42.5%	9.7%
	# Breaches =614	# Records = 92M	# Breaches =783	# Records = 85.6M

Data Breach Category Summary for 2013 and 2014 [Source: ITRC, 2014]

The overall cost of cybercrime and cyberattacks is staggering. According to Watkins (2014), the annual cost of cybercrime has been estimated to be $385 billion around the globe, however, businesses in some nations are more likely to be the target of such crime. “The UK National Audit Office estimates cybercrime costs the UK between 18 billion ($30 billion) and 27 billion (45 billion) a year. In the US that figure is estimated to be roughly $100 billion” (Watkins, p. 2-3).

Organizations in the United States are significantly more likely to be the targets of cybercrime. In 2013, 54% of cyberattacks targeted an entity in the US (Watkins, 2014). U.S. Homeland Security estimates over 1,000 US businesses have been infected by malware that captures customer payment information (Perlroth, 2014). Home Depot’s data breach reported in early September of 2014 added to a growing list of US retailers that had been victims of such breaches, including U.P.S., Target, Michael’s, eBay and Neiman Marcus.

LITERATURE REVIEW

Data Breaches

Costs to the organization/data handlers

Costs to an organization that has been a victim of a cyberattack vary depending on the extent of the breach and a number of other factors. However, Malecki (2014) offers some averages for the costs. He reports that in 2011 the Poneman Institute interviewed officials at 49 companies that had been the victim of an attack that led to the loss of customers’ data. The results found that the average total cost of a data breach was $5.5 million. This included losses in revenue as well as the costs associated with dealing with the breach. These figures are based on breaches that occurred up to 2011.

As noted earlier, the frequency and intensity of the breaches has been increasing rapidly. For example, Lafuente (2014) argues that the pervasive use of “big data” has led to even larger damage from data breaches, because of the large amounts of data that are now stored. As the number of records stored/released increases, so does the cost of responding to a breach. Pearson (2014) notes that one of the primary costs in responding to a crisis is the requirement to notify the individuals whose data has been compromised. “For a business that operates online, such as a retailer, the costs of informing all their customers alone could be crippling”(p. 12). Kumar (2014) reports that companies based in the US paid an average of $246 per record that was compromised in the data breach. As the number of records and the frequency of attacks continues to grow, so do the costs for companies.

However, the costs to the company are not strictly in monetary terms. “Cyber attacks can cause significant loss of business intelligence and intellectual property, drive up the cost of security, disrupt workflow, and damage company reputation. Companies reporting major attacks suffer a 1-5% drop in stock value, while some companies recover, others lose everything” (Watkins, 2014, p. 3). What is not commonly understood is that the majority of those costs in the private sector may come from the loss of intellectual property, which is estimated to account for three-fourths of the losses (Watkins, 2014).

Costs of data breaches are tangible and intangible

Certainly for an organization there are both tangible and intangible negative aspects of data breaches. The costs an organization pays to inform customers or the fines to be paid are tangible. However, an organization can also incur intangible harm to their reputation, image and brand. The same can be said for the individuals who have their information released. There are the tangible costs of repairing damage to your identity, as well as intangible costs to the individual's state of mind.

Acqulisti (2014) argues that the harms faced by individuals who have had personal information breached should be thought of as being exposed to subjective harms and/or objective harms. Subjective harms are those anticipated perceptions of harm. "Subjective harms include anxiety, embarrassment, or fear; the psychological discomfort associated with feeling surveilled; the embarrassment associated with public exposure of sensitive information; or the chilling effects of fearing one's personal life will be intruded upon" (p. 83). Subjective harms are difficult to quantify. Objective harms, on the other hand, are "the unanticipated or coerced use of information concerning a person against that person" (Acqulisti, 2014, p. 83). They would include incidents of high harm (identity theft) or low harm (spam emails or junk mail). There is also the issue of the probability of a harm occurring. While the probability of getting more junk mail may be high, the probability of the high harm of identity theft is relatively small.

Havov's and Gray's (2014) stakeholder analysis of the breach at TJX, an American apparel and home goods company, divided the consumers whose information was disclosed into three distinct groups. First, were the consumers who suffered identity theft resulting in financial and more subjective harms. Second, were the consumers whose credit card information was leaked, but was never used. These consumers suffered no objective, financial harm, but they may have been subjected to, in Acqulisti's (2014) taxonomy, subjective harm associated with the anxiety. This second group was very large. The final group of consumers discussed by Havov and Gray were those who took advantage of the special discounts offered by TJX. Not only did they suffer no objective harm from their information being leaked, but they also benefited from the special discounts provided. Thus, Havov and Gray would argue that those individuals who have had their personal information leaked should not be thought of as a single, cohesive group.

Responses to increasing threat of cybercrime

It was inevitable that there would need to be responses to deal with the increasing number of data breaches. These responses have materialized on several levels. There have been responses by governments, organizations who handle the data and by individuals.

An obvious response to the threat of a cyberattack is to increase the organization's e-security. Kumar (2014) reported the results of a survey of IT professionals saying that only 37% thought their organization was building products with security in mind. The biggest reasons for failing to increase security were a lack of management approval, training and support. However, the same report found that the security of websites has been increasing, with the number of serious vulnerabilities dropping from 1,000 per site in 2007 to 56 per site in 2012. Yet, the vulnerabilities remain.

In addition to increasing their security procedures, many businesses are now buying insurance to help them recover from a cyberattack. Perlroth and Harris (2014) found that specialized polices that deal with cyberattacks are being offered by about 50 carries and that demand for those policies is increasing. They noted that demand for the policies increased 21% from 2012 to 2013 alone. All of these policies are leading to increased premiums – from $1 billion in 2012 to #1.3 billion in 2013.

Watkins (2014) also reports significant growth in the purchase of insurance for cyberattacks. However, he notes that such insurance has limits. While the insurance can help an organization to repair the systems and recoup the costs of dealing with the breach, most policies do not compensate the company for the loss of intellectual property. Malecki (2014) reports the results of a study of insurance payouts from 137 cyberattacks between 2009 and 2011. The study by NetDiligence found that the average total payout per event was $3.7 million. Of that figure payouts in legal settlement per event was $2.1 million and for legal defense it was $582,000.

As the number and magnitude of data breaches has grown, nations and many US states have moved to pass legislation for the protection of individuals. These laws all vary in the actions required. However, according to Pearson (2014), the laws tend to give regulators more power and make the data handlers more liable, as evidenced by larger fines being allowed, greater regulation, and requirements for the notification of individuals whose data was compromised. However, Kumar (2014) notes that companies operating in the European Union are required by EU regulations to provide an appropriate level of protection of consumer data against cyberattacks. The US has no similar requirement, although, as noted above, individuals may turn to the courts for restitution. Kumar also notes that China has taken a more proactive approach by "…restricting use of certain applications and products in order to safeguard themselves from cyber threats" (4).

Data breaches involving health information are not exempt from potential litigation, despite the fact that federal HIPPA rules do not allow individuals to bring an action for such a breach. Individuals can simply use state laws or torts to bring "… a steady stream of primarily data-breach cases being filed in state courts" (Terry, 2014, p. 838).

Crises and Crisis Response Strategies

For the organization and the individuals involved, data breaches can easily constitute a crisis in many ways. Coombs (2014) defines a crisis as "…a significant threat to operations or reputations that can have negative consequences if not handled properly." The main concern in any crisis is public safety. Public safety includes the potential of psychical, emotional, mental, and financial harm to members of the public (2014). Crisis management is designed to control the crisis and defend the stakeholders and organization from potential harm.

Crisis management is divided into three main sections: pre-crisis, crisis response, and post-crisis. The pre-crisis phase is intended to prevent a crisis, but also should contain several pretested crisis communication materials (press releases, dark websites, statements, etc.). The crisis response phase involves responding to the crisis in an effort to control damage to stakeholders and the organization. The post-crisis phase involves learning from the mistakes made that led to the crisis. Also, providing follow-up information to the public and return to business as usual (Coombs, 2014).

In any crisis, the organization involved needs to respond. Responses must be well planned and strategic. The first stage of a crisis response is the initial response. Coombs (2014) outlines three important elements of the initial response: be quick, be accurate, and be consistent. The most effective communication during a crisis is face-to-face (FTF), which means the CEO, or other spokesperson, should be prepared to do a press conference or release a video statement within an hour after a crisis starts or is announced (Nikolaev, 2010).

Not only is it important to have a response within the first hour of a crisis, but also to be available to the media. If the organization does not talk to the media, other people will talk to the media, and the organization will lose its power to tell the story. Coombs describes a crisis causing a vacuum. The media will rush to suck up any information possible, especially with the advent of social media (2014).

"Stealing Thunder" in crisis communication is a relatively new strategy that involves an organization reporting the crisis to the public before news media can report the story. The practice of stealing thunder comes from law, when a defendant reports damaging information, instead of the prosecution (Williams, Bourgeois & Croyle, 1993). The idea is that the defendant looks more honest, and can possibly sustain less damage by self-reporting (Arpan & Roskos-Ewoldsen, 2005; Claeys & Cauberghe, 2012).

All facts that can be disclosed should be disclosed to an organization's publics when releasing information during a crisis (Nikolaev, 2010). Besides making a spokesperson seem untrustworthy, hiding facts or keeping information from the public can damage the reputation of an entire organization. Responses should include "what happened, when, where, who, and how many people are involved, what is being done, and what kind of and when first recovery results can be expected," (Nikolaev, p. 273). Disclosing information shows that the organization has taken control to fix problems and gives people hope that the issues will be resolved. In the event that the crisis management team does not have all of the information by the time a response should be given, the spokesperson should only disclose information that is known for sure. According to Nikolaev, the organization's spokesperson should follow three basic rules: "do not go off record, do not speculate, do not disclose liability," (2010, p. 274).

During a crisis, an organization should not be endorsing itself through advertising or other forms of promotion. Commercials and advertisements should be removed from all media, as dealing with the crisis should be the top priority. Nikolaev uses the example of an airline crash: "it is not a time to show people safely flying with your company and happily eating peanuts," (2010, p. 272).

Websites are a major channel of communication for organizations. Organizations can control the information being posted, offer a central location for stakeholders to gain information, and information can be posted and updated quickly. A growing and large segment of the population turns to organization's websites for relevant and updated information (Holcomb, Gottfried & Mitchell, 2013).

The use of social media to respond to a crisis has proven to be a new and useful tool to organizations. According to Holcomb, et al. (2013), social media allows for immediate and updated messages delivered to the masses. Also, social media allows for consumers to directly respond and communicate with the organization, creating a dialogue between the impacted group and the organization.

After the initial response has taken place, the next step is to start rebuilding the organization's reputation. This goal is achieved in a variety of ways. Listed below are the top strategies discussed by Coombs (2014).

1. Attack the accuser: crisis manager confronts the person or group claiming something is wrong with the organization.
2. Denial: crisis manager asserts that there is no crisis.
3. Scapegoat: crisis manager blames some person or group outside of the organization for the crisis.
4. Excuse: crisis manager minimizes organizational responsibility by denying intent to do harm and/or claiming inability to control the events that triggered the crisis.
   Provocation: crisis was a result of response to someone else's actions.
   Defeasibility: lack of information about events leading to the crisis situation.
   Accidental: lack of control over events leading to the crisis situation.
   Good intentions: organization meant to do well
5. Justification: crisis manager minimizes the perceived damage caused by the crisis.
6. Reminder: crisis managers tell stakeholders about the past good works of the organization.
7. Ingratiation: crisis manager praises stakeholders for their actions.
8. Compensation: crisis manager offers money or other gifts to victims.
9. Apology: crisis manager indicates the organization takes full responsibility for the crisis and asks stakeholders for forgiveness.

The preceding list provides several common strategies used by crisis management practitioners. Attribution to a crisis is a major concern in crisis management. People tend to attribute a crisis to an organization or a situation. It is important for crisis management practitioners to try to place the attribution on the situation, rather than the organization. If attribution to a situation is done properly, organizations can avoid lasting damage to the brand, loss of potential sales, and negative word-of-mouth (Coombs & Holladay, 2006).

Expressing concern for stakeholders during a crisis is crucial. Whether the crisis is the organization's fault or due to an outside source, expressing concern can not only help lessen the damage to an organization's reputation, but it can also reduce financial loss following an incident and reduce the number of lawsuits against an organization (Cohen, 1999; Kellerman, 2006). Constructing an effective message of concern should be done as soon as possible after a crisis occurs to let stakeholders know that the organization is apologetic and cares for them. Without this message, the publics may think the organization does not care, which can further damage a reputation (Hearit, 2007).

Keeping the spokesperson in the public eye is important in both the crisis-response phase and the post-crisis phase. This means that it is a good idea to schedule press conferences throughout the crisis in to ensure FTF communication from an organization to its publics and to provide updates on the crisis. If the CEO is the spokesperson, he or she should be delivering updates to show the organization's high level of involvement in the crisis and to provide credibility and expertise (Nikolaev, 2010). An organization needs to inform its publics with as much information as it can disclose as soon as that information is available. By being open and honest throughout a crisis, an organization lessens the chance of long-term damage on its reputation.

During a crisis, it is important to monitor what the public and the media are saying about the crisis and those involved. Monitoring involves keeping track of media coverage and the public's reaction to the crisis team's efforts (social media posts, comments on new stories, etc.) Once a crisis has been resolved, use the media coverage and responses as tools for learning (Nikolaev, 2010). Perhaps the statements that had been pre-drafted were not accepted favorably by the public, or maybe the CEO could not deliver messages in an effective way. Organizations can analyze what happened to see what worked and what did not. If improvements need to be made, then the crisis plan should be updated to reflect the changes (Coombs, 2014).

The previous review of literature notes that data breaches are a significant problem for organizations and the problem is growing. The purpose of this research project is to determine current strategies used by organizations to respond to crises caused by data breaches. Due to the exploratory nature of this research, the project was designed to attempt to answer the following research questions.

RQ1: To what extent do organizations use Coombs' crisis response strategies in their data breach crisis response?
RQ2: Are there additional response strategies or content employed by organizations in response to data breaches?
RQ3: What attributions do organizations make in their data breach crisis responses?

METHODS

Selection of Data Breaches

The selection of data breaches was made possible through the work of the Identity Theft Resource Center. On January 15, 2015 the Identity Theft Resource Center published a report consisting of all the known data breaches that took place in 2014. The breaches were broken into five different industry groups: Banking/Credit/Financial, Business, Educational, Government/Military, and Medical/Healthcare. We then chose to research the top two categories based on the number of records breached. The Business category contained 68,237,914 records breached in 2014, followed the Healthcare/Medical category containing 8,277,991 records breached during the same year.

Because they impacted the most individuals and also were most likely to have an official organizational response, the top ten organizations in terms of records breached for the business and healthcare/medical categories were chosen for analysis. Due to the lack of access to an official organization response statement from one organization in the business category and two in the health care category, we expanded our analysis to the top 11 breaches in retail and top 12 in health care. The result was an analysis of the top ten organizational responses for each category that were available for analysis. Table 1 lists the top data breaches in the medical and retail categories for which the official statement was analyzed in this research.

Table 1. Top data breaches in retail and health care sectors during 2014 for which an official response could be found and were included in the study.

Business/Retail Organizations	Date of Breach	#of Records Exposed
Home Depot	April & September 2014	56 million
Michael's	May 8, 2013 to January 27, 2014	2.6 million
Staples	August 10, 2014 to September 16, 2014; and July 20, 2014 to September 16, 2014	1.16 million
Neiman Marcus	July 16, 2013 to October 30, 2013	1.45 million
Goodwill	February 10, 2013, to August 14, 2014	868,000
Variable Life Insurance	Thursday, October 25, 2007	774,723
Spec's	October 31, 2012 through March 20, 2014	550, 000
Paytime, Inc	April 7 to April 20, 2014	233,000
Aaron Brothers	June 26, 2013 to February 27, 2014	400,000
Walgreens	March 3, 2014 to April 14, 2014	160,000
UPS	January 20, 2014 to August 11, 2014,	105,000
Health Care Organizations		
Community Health Systems / Tennova /Complete Heal	April & June 2014	4.5 million
St. Joseph Health System	December 16 to December 18, 2013	405,000
Sutherland Healthcare Solutions	February 5, 2014 to March 7, 2014	342,197
Touchstone Medical Imaging, LLC	May 9, 2014 to September 5, 2014	307,528
Indian Health Service – Maryland	August25, 2014, to August 29, 2014	214,000
Barry University (Foot and Ankle Institute)	May 14, 2013	136,000
Community Health Center	January 1, 2014	130,000
NRAD Medical Associates, P .C.	April 24, 2014	97,000
Patient Care Services at Saint Francis, Inc.	January 1, 2011	84,000
Aventura Hospital and Medical Center	September 13, 2012 – June 9, 2014	82,601
Central Dermatology	August 9,2013 to September 25, 2014	76,258
Visionworks	October27, 2014	74,944

Analytical Tool

After selecting the data breach cases to be analyzed, we developed an analytical tool using the response strategies found in Coombs' Crisis Management and Communication (2014). Coombs presented and defined twelve response strategies typically used in crisis communication, which led to the building of our code sheet. The response strategies were described in the review of literature and are also listed on Table 2. After analyzing twenty organizational responses to the data breach, we found several common categories of content. The discovery of eight new content categories led to the development of a second code sheet that was comprised of the content categories. The content categories are identified in Table 3, discussed below.

Coding

The format for the organization's response varied. Some organizations communicated with a letter, while others issued a statement or a press release. Two individual coders analyzed each message sentence-by-sentence, looking for response strategies defined by Coombs. If the message contained a response strategy, the coder would directly copy the content and place it in the code sheet with the corresponding strategy. After the two individuals coded the twelve communication messages independently, the coders compared the code sheets. In the few instances of disagreement between coders the coders discussed the category and recoded.

After the initial coding, we found that our code sheet based on Coombs' response strategies did not account for eight common content categories that appeared in many of the messages from the organizations. This led to the implementation of a second code sheet to account for those categories. Again, the coders independently analyzed the messages and copied the content found in the message and placed it in the code sheet with the corresponding strategy. Next, the two coders compared and merged their finding into one code sheet.

Inter-coder Reliability

Coding of th**e** initial communication from the organization was separated into two sectors, business retail and healthcare. A team of two was assigned to code the available, official response from top ten healthcare and business retail data breaches. Each team member individually coded the response and used the twelve response strategies identified by Coombs. If the coder found a response strategy, they directly copied the content and placed it in the code sheet with the most fitting Coombs response strategy. After individually coding, each team attempted to create on final coding sheet. The inter-coder reliability was very high, with a 87% agreement between the healthcare response coders. The business retail coders also shared a high level of agreement, citing 91% agreement. Each team of coders negotiated amongst themselves, and easily created one, final code sheet was used for the results in the next section.

RESULTS

The results section presents the results of the coding of the top-10 corporate responses to data breaches in the retail and health-related sectors. The presentation of the results follows the research questions posed earlier.

RQ1. To what extent do organizations use Coombs' crisis response strategies in their data breach crisis response?

Table 2 presents the frequency counts for the 12 strategies identified by Coombs. The results identified four commonly used strategies, one strategy that was used one time and the remaining seven strategies were not identified in any of the 20 official response statements from the organizations.

Table 2. Use of Coombs' Response Strategies in Data Breach Crisis Response Strategies

Strategy	Health Org	Retail Org	Row Total
Scapegoat	7	10	17
Compensation	10	7	17
Justification (minimize)	9	7	16
Apology	9	7	16
Reminder	0	1	1
Attack the Accuser	0	0	0
Denial	0	0	0
Ingratiation	0	0	0
Excuses			
Provocation	0	0	0
Defeasibility	0	0	0
Accidental	0	0	0
Good intentions	0	0	0
Column Total	35	32	67

The results make it clear that four strategies were in favor when organizations respond to a crisis from a data breach. In 17 of the 20 cases studied the strategies of scapegoating and compensation were employed. In 16 of the 20 cases the strategies of justification/minimize and apology were employed. Each of these four strategies is discussed in greater detail below.

Scapegoating. Since the vast majority of the breaches were the result of actions of individuals outside of the organization, it was easy for organizations to use scapegoating. The statement of the Indian Health Services of Maryland noted that "a physician employed by a staffing company under contract with the IHS had improperly accessed protected health information from three IHS facilities." A statement in the official press release of UPS regarding their data breach named the scapegoat as "malware." In a letter to the parents of minors whose information may have been compromised, St. Joseph Health Systems said, "SJHS experienced a security attack in which hackers gained unauthorized access to one server on its computer system." Malware and/or hackers were the most common groups identified as the scapegoats.

Compensation. All ten of the health organizations and seven of the retail organizations offered compensation to those effected by the data breach. In all cases, the compensation offered to those effected was some form of credit monitoring service. For example, "The Home Depot continues to offer free identity protection services, including credit monitoring, to any customer who used a payment card at a Home Depot store in 2014, from April on." Most organizations provided at least a brief description of the free services being provided as well as information on how to contact the organization providing those services (e.g. ID Experts, AllClearID and Experian).

Justification/Minimize. In 16 of the 20 cases coded, the official statement of the organization included efforts to minimize the extent of the crisis. As noted in the literature review, much of the harm associated with a data breach is the anticipation that your information will be used by others, as opposed to the actual theft of an identity. It is possible that the individuals crafting these official responses were attempting to alleviate some of that anticipation by noting the minimal risk involved. In some cases organizations chose to minimize the risk by noting that very sensitive information was not exposed. For example, Home Depot noted that the files taken "…did not contain passwords, payment card information or other sensitive personal information." Other organizations noted that there had been no reports of the misuse of the data. Touchstone Medical Imaging said, "We have no knowledge and there is no indication that any of your information has been used improperly. However, we are now sending you this letter in an abundance of caution to let you know this happened." Barry University's Foot and Ankle Institute said, "To date, Barry University is not aware of any reports of identity fraud, theft, or other harmful activity from this incident."

Apology. Whether the organization attributed the cause of the breach to external sources or not, 16 of the 20 cases reviewed included an apology. The Variable Life Insurance company echoed the words of many of the statements when it said, "We value the trust you have placed in our company and apologize for any concern this matter may have caused you." Those words were echoed by Spec's, the online glasses company, when they said, "We are deeply distressed about this incident and sincerely apologize for the worry and convenience this may cause you."

The organizations chose not to employ the attack the accuser or denial strategies. It is likely that this decision is based on the fact that often the notification of the data breach came from official sources or the organization itself, so these strategies would likely be counterproductive. The two similar strategies of reminding stakeholders of past good deeds and ingratiation were only employed in one case of the 20. Only one organization (Goodwill) chose to remind stakeholders of its past good deeds. Given the mission of Goodwill Industries, such a reminder was an appropriate choice. However, for for-profit organizations that could attribute the cause externally, there likely was little incentive to use the strategies discussed thus far.

Interestingly, there were no examples of excuses being made. Again, the fact that most of these crises had external causes may have meant there was no need to offer an excuse. It should be noted that in the initial coding, 20% of the cases were coded as having offered a provocation excuse. However, after the discussion among the coders, during the second coding it was determined that those provocation statements were actually examples of scapegoating alone. The coders noted that given the data breach cases under analysis, that there appeared to be few substantial differences between the scapegoating strategy and the provocation excuse.

The results for the first research question note the overwhelming use of four of Coombs' strategies when responding to data breach crises. It is interesting to note that the results in table 2 make it clear that for the cases examined there were no significant differences in the selection of response categories dependent on the industry. The four response categories were the same for both health and retail organizations, and they were used in nearly identical amounts.

RQ2. Are there additional response strategies or content employed by organizations in response to data breaches?

In addition to applying the Coombs' strategies to responses for data breach crises, the current investigation also looked for additional content that was commonly used across the response categories. Table 3 provides the data for the most common content elements identified by the coders. In all 20 of the official organizational statements there was a description of the type of data that had been breached. The statements also included description of what steps the organization took immediately upon disclosure (17), expressions of the organization's commitment to the security of information (16) and the explicit statement of a phone number to speak to someone for further information (15). Expressions of the organization's commitment to security were often tied to apologies.

Table 3. Eight Recurring Content Elements in Responses

Recurring Content Elements	Health Org	Retail Org	Row Total
Present information on the type of data breached	10	10	20
Describe the immediate actions taken by the company	8	9	17
Express their commitment to security and/or privacy of information	7	9	16
Provide a call center for questions.	9	6	15
Note that they are/have been working with law enforcement	6	8	14
Suggest additional strategies for protecting their credit/identity	8	6	14
Describe future actions to be taken	9	2	11
Provide details on compensation (credit monitoring, etc.)	3	7	10
Column Totals	60	57	117

Over one-half of the official statements analyzed included content noting that the organization was or had worked with law enforcement (14), provided additional strategies for protecting the customer's credit or identity (14), described future actions the organization would be taking (11) or provided additional details regarding compensation, including the offer to provide free credit monitoring services (10). The eight recurring content elements listed on table 3 provide organizations a list of the most commonly used content across the health and retail organization examples analyzed.

RQ3. What attributions do organizations make in their data breach crisis responses?

Previous research has found that the attribution of the source of the crisis can play a role in the selection of the appropriate response strategy. To ascertain the attribution the coders also determined if the official organizational response attributed the source to the organization or to some external factor. For the coding, attributions to the organization in general or an employee of the organization were viewed as internal/organizational attribution.

The results of the current research demonstrate that in the case of data breaches the vast majority of the attributions are to external sources. Table 4 presents the counts for the attribution in terms of the health care and retail organizations. It is important to note that in all cases it was possible for the coders to ascertain the organization's attribution. The three internal references in the health care category included a reference to an employee by job title (radiologist) and two references to an unnamed employee who had done something to cause the breach. The only incidence in the retail category of an internal attribution was to an unnamed employee. Eighty percent (16) of the attributions were to external factors and the vast majority (12) named hackers or malware. The focus on hackers and malware is expected given the nature of the crises. Other external factors included contract employees (2), a former employee and computer thieves. Both incidences of contract employees as an external agent appeared in the health care industry, an industry category where contracting workers from another organization is more common.

Table 4. Crisis Attribution by Industry

Attribution	Health Org	Retail Org	Row Total
Organization/Internal	3	1	4
External	7	9	16

DISCUSSION & CONCLUSIONS

The current research found that almost all 20 of the businesses studied had used at least one or more of the following crisis response strategies: scapegoating, compensation, justification/minimization, and/or apology. Because data breaches have become a more common problem in recent years, it is likely that affected businesses will continue to use these response strategies when providing customers with information following a breach. Combined, the strategies mentioned can be a basic "guide" for businesses dealing with a data breach.

Previous crisis communication research has identified 12 common response strategies. However, this study found that of the list of Coombs' 12 crisis response strategies, the four strategies mentioned in the previous paragraph are the most effective to use when dealing with a data breach. Because data breaches are a relatively new problem, there is little research pertaining to how businesses can, and should, respond.

In addition to the four strategies commonly employed, the current investigation also identified eight types of content that commonly appear in data breach responses from organizations in the business and healthcare sectors that were studied. These recurring content elements are presented in table 3, and they also offer guidelines about what types of content are likely to be included in the organization's response to a data breach. The eight content categories are used in one-half or more of the organizational responses studied.

Although the study found that there are a number of response strategies that are used almost universally when dealing with a data breach, further research can be done on this subject. This research examined breaches that occurred in 2014 in the healthcare and retail industries. Future investigations could include different industries that have been affected, more years of breaches, and more than the top ten largest breaches per year. Future research could also be expanded to feature response strategies from multiple sources including social media, letters to customers, and website posts, as opposed to looking at a single official organizational response.

REFERENCES

Acqulisti, A. (2014). The economics and behavioral economics of privacy. In J. Lane, V. Stodden, S. Bender. & H. Nissenbaum. (Eds.), *Privacy, big data, and the public good: frameworks for engagement* (pp.76-95). New York, NY: Cambridge University Press.

Arpan, L. M., & Roskos-Ewoldsen, D.R. (2005). Stealing thunder: an analysis of the effects of proactive disclosure of crisis information. *Public Relations Review 31*(3), 425-433.

Claeys, A. S., & Cauberghe, V. (2012). Crisis response and crisis timing strategies, two sides of the same coin. *Public Relations Review, 38*(1), 83-88.

Cohen, J. R. (1999). Advising clients to apologize. *S. California Law Review*, 72, 1009-131.

Coombs, W. T. (2014). Crisis Management and Communications. *Institute for Public Relations*. Retrieved from http://www.instituteforpr.org/crisis-management-communications/

Coombs, W. T. & Holladay, S. J. (2006). Halo or reputational capital: reputation and crisis management. *Journal of Communication Management, 10*(2), 123-137.

Dwyer, C. E. (2014). Effectiveness of data breach legislation, 2005-2012. Thesis – Georgetown University, Masters in Public Policy.

Frei, S. (2014). *Why your data breach is my problem*. NSS Labs.

Hearit, K. M. (1994, Summer). Apologies and public relations crises at Chrysler, Toshiba, and Volvo. *Public Relations Review, 20*(2), 113-125.

Havov, A., & Gray, P. (2014). The ripple effect of an information security breach event: a stakeholder analysis. *Communications of the Association for Information Systems, 34*, 893-912.

Holcomb, J., Gottfried, J., & Mitchell, A. (2013). News use across social media platforms. Washington, DC: Pew Research Center. Retrieved from http://www.journalism.org/files /2013/11/News-Use-Across-Social-Media-Platforms1.pdf

Identity Theft Resource Center - ITRC. (2013). *Data breach reports*. Retrieved from: http://www.idtheftcenter.org/ITRC-Surveys-Studies/2013-data-breaches.html

Identity Theft Resource Center - ITRC. (2014). *Data breach reports*. Retrieved from: http://www.idtheftcenter.org/images/breach/DataBreachReports_2014.pdf

Kellerman, B. (2006, April). When should a leader apologize and when not? *Harvard Business Review, 84*(4), 73-81.

Kumar, N. (2014). *Today's importance of cybersecurity.* (Unpublished doctoral dissertation). Retrieved from ProQuest Digital Dissertations. (UMI1571407)

Lafuente, G. (2015). The big data security challenge. *Network Security, 2015*(1), 12-14.

Malecki, F. (2014). The cost of network-based attacks. *Network Security, 2014*(3), 17-18.

Nikolaev, A. G., (2010). Thirty common basic elements of crisis management plans: Guidelines for handling the acute stage of "hard" emergencies at the tactical level. *In:* W. T. Coombs, and S. J. Holladay. *The Handbook of Crisis Communication.* (pp. 261-281) Singapore: Blackwell Publishing.

Pearson, N. (2014). A larger problem: financial and reputational risks. *Computer Fraud & Security, 2014*(4), 11-13.

Perlroth, N. (2014, October 2). Home depot data breach could be the largest yet. *The New York Times.* Retrieved from http://bits.blogs.nytimes.com/2014/09/08/home□depot□confirms□that□it□was□hacked/?module=Search&mabReward=relbias%3Aw

Perlroth, N., & Harris, E. A. (2014, June 8). Cyberattack insurance a challenge for business. *The New York Times.* Retrieved from http://www.nytimes.com/2014/06/09/business/cyberattack-insurance-a-challenge-for-business.html?_r=0

Terry, N. (2014). Health privacy is difficult but not impossible in a post-HIPAA data-driven world. *Chest, 146*(3), 835-840.

Watkins, B. (2014). The impact of cyber attacks on the private sector. Paper presented at conference of the *Association for International Affairs.* Retrieved from http://www.amo.cz/publications/the-impact-of-cyber-attacks-on-the-private-sector.html?lang=en#.VREBgjTF9Wa.

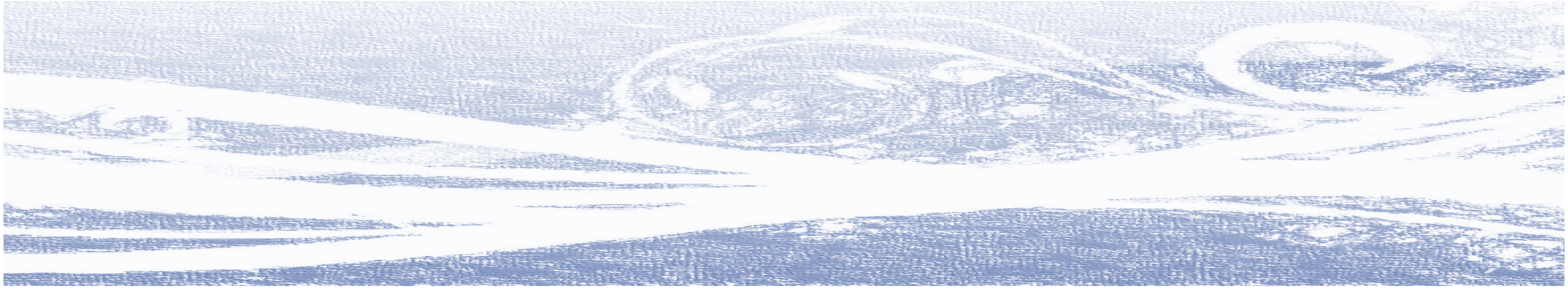
Williams, K. D., Bourgeois, M. J., & Croyle, R. T. (1993). The effects of stealing thunder in criminal and civil trials. *Law and Human Behavior*, *17*(6), 597.

QRBD

QUARTERLY REVIEW OF BUSINESS DISCIPLINES

August 2016

Volume 3
Issue 2



A JOURNAL OF INTERNATIONAL ACADEMY OF BUSINESS DISCIPLINES
SPONSORED BY UNIVERSITY OF NORTH FLORIDA
ISSN 2334-0169 (print)
ISSN 2329-5163 (online)