2015

The great data breach

De'Andre M. Brown

The great data breach

Abstract

This paper examines how Target Corporation dealt with their data breach when their network was infiltrated by hackers compromising the debit and credit card information of millions of customer's personal information including customer names, mailing addresses, phone numbers and e-mail addresses. Crisis communication models that are used to evaluate the effectiveness of corporations' handling crisis situations in a world where social media and speed dominate the news cycle.

Degree Type

Open Access Senior Honors Thesis

Department

English Language and Literature

First Advisor

Regina Luttrell

Second Advisor

Mary K. Ramsey

Keywords

crisis management, social media, data breach, disaster management, data intrusion, crisis communication

THE GREAT DATA BREACH

By

De'Andre M. Brown

A Senior Thesis Submitted to the

Eastern Michigan University

Honors College

in Partial Fulfillment of the Requirements for Graduation

with Honors in ___English Language & Literature____

Approved at Ypsilanti, Michigan, on this date September 23, 2015

The Great Data Breach

De'Andre Brown

Eastern Michigan University

ABSTRACT

This paper examines how Target Corporation dealt with their data breach when their network was infiltrated by hackers compromising the debit and credit card information of millions of customer's personal information including customer names, mailing addresses, phone numbers and e-mail addresses. Crisis communication models that are used to evaluate the effectiveness of corporations' handling crisis situations in a world where social media and speed dominate the news cycle.

Keywords: Crisis management, crisis communication, data breach, communication theory, the Situation Crisis Communication Theory

INTRODUCTION

We live in a time when the chances of a crisis erupting is predictably high. It seems as though we are becoming immune to reading headlines about another large company's computer system being hacked revealing a variety of personal data about their customers. From emails to phone numbers, credit cards and scores of social security numbers, today's customer information is at risk. This paper examines how Target Corporation, one of the largest companies in the United States, handled an unprecedented computer Breach. Crisis communication models that are used to evaluate the effectiveness of corporations' handling of crisis situations are explored.

In order to understand the field of Crisis Communication it is important to define what a crisis is, understand the history of crisis and understand the importance of organizations having a crisis management plan. Throughout the history of crisis communication, scholars and practitioners sought to create a standard definition for crisis, but no one universal definition exists. Communications expert Kathleen Fearn-Banks defines a crisis as, "a major occurrence with a potentially negative outcome affecting the organization, company or industry, as well as its publics, products, services, or good name."(Fearn-Banks, 2011). Timothy Coombs goes on to assert that a crisis is, "the perception of an unpredictable event that threatens important expectations of stakeholders and can seriously impact an organization's performance and generate negative outcome" (Coombs, 2012). The word crisis can be applied to a multitude of situations some of which have plagued the United States and formed the need for crisis management.

Crisis management is the overall pre-established procedures outlined for preparing or responding to cataclysmic events or incidents in a safe and effective manner (Society for Human Resources Management, 2005). Crisis management "involves planning, organizing, leading, and

controlling assets and activities in the critical period immediately before, during and after an actual or impending catastrophe to reduce the loss of resources essential to the organization's eventual full recovery" (NyBlom, Reid, Janine, Williams, & Walter, 2003). Crisis management is a challenge any organization can encounter, and many fail (Coombs, 2012). This is a direct result from the unpredictability of crises situations and then organizations being ill prepared. When an organization is not prepared for a crisis, publics and stakeholders suffer because of the organizations inability to protect its assets and failure to communicate how publics and stakeholders can protect themselves. The purpose of crisis communication is to outline a strategic communication plan that identifies key members of a crisis management team and important publics that will need to be communicated with (NyBlom, Reid, Janine, Williams, & Walter, 2003). With recent data breaches happening in the retail, finance, postal services, and restaurant industries the importance of crisis communication plans are becoming more evident. Organizations are clamoring to prevent security breaches. The purpose of this paper is to benchmark best practices and to analyze the overall crisis communication strategies used by Target Corporation comparing its practices to best practices outlined by scholars and practitioners of crisis communication. With majority of scholars focusing on the prevention and recovery of the crisis communication plan, this research will primarily focus on the following:

- crisis response strategies used by organizations to communicate to publics and stakeholders the effects of the crisis;
- the ability to update publics and stakeholders throughout the crisis; and
- the strategies used during the recovery phase to return the organization back to normal or create a new norm.

Three pivotal case studies will be used as the benchmark in this research. Johnson & Johnson 1980, Exxon Valdez 1989 and Domino's (2009) will be used as exemplars to illustrate communication strategies that should or should not be used in crisis communication. These cases along with best practices will serve as the benchmark for evaluating the response strategies of Target Corp. used to respond to recent data breaches.

LITERATURE REVIEW

Crisis communication "is the dialog between the organization and its public(s) prior to, during, and after the negative occurrence." Further, it details strategies and tactics designed to minimize damage to the image of the organization (Fearn-Banks, 2011). Crisis that occurred for Johnson & Johnson and Exxon are vital to this research because they exemplify what we have come to understand as traditional methods of communicating during a crisis prior to social media. Both crisis occurrences symbolize the importance of an organization having an effective crisis communication plan. The crisis that befell Domino's Pizza reminds us that crises can occur at any time and organizations must swiftly gather details and actively respond to the crisis. Additionally, the importance of organizational monitoring and understanding the importance of having social media are integral in the overall communication strategy of today's crisis.

Johnson & Johnson

Johnson & Johnson historically has been an organization that was trusted by consumers for the quality in products like baby products, lotions, shampoos, cotton swabs, toothbrushes, and surgical instruments. In fact, the company is often considered a household name. Ranked the top 100 best places to work by employees and aligned themselves with four responsibilities: to the consumer, to the employer, to the communities, and to the stakeholder. Because of their strong

relationship with the media, the organization became suspicious when a reporter from the Chicago Sun contacted them on September 30, 1982 asking for background information on Tylenol, a medication used to alleviate pain.

The reporter who originally contacted Johnson & Johnson was assigned by an editor to collect background information on the over the counter drug. The information collected by this reporter was used as part of the lead story which revealed that multiple customers died after consuming Johnson & Johnson's Extra Strength Tylenol brand.

The first step in responding to the crisis was when Robert Andrews, assistant director for public relations at Johnson & Johnson was notified that a reporter was seeking information about a link between the deaths and the company's product. Andrews recalls how the company reacted in the first days of the crisis: "We got a call from a Chicago news reporter. He told us that the medical examiner there had just given a press conference-people were dying from poisoned Tylenol. He wanted our comment. As it was the first knowledge we had here in this department, we told him we knew nothing about it. In that first call we learned more from the reporter than he did from us" (Berge, 1990)

During this time the organization did not have a specific crisis management plan and the leaders of the organization feared the worse. There were no prodromes explaining how to appropriately handle the crisis, because nothing of its kind ever occurred amongst themselves or competitors. After receiving the news CEO James Burke held a meeting with top executives and began dispatching leaders to parts of the organization to find out what happened. Fearn-Banks (2011) notes that this would have been the second step of the crisis communication plan-had there been such a plan.

When the story ran in the media it sparked fear amongst the general public, because most people were afraid they could possibly die from taking a capsule for a headache. While having no crisis management plan in place, David Collins, chairman of McNeil assembled a seven member crisis team to help investigate the crisis and determine the proper strategies to be taken to mitigate the crisis. Their top priority was to protect consumers and then save the product. The crisis team had the authority over all communication that would happen on the behalf of the organization and there first order was to recall the Extra Strength Tylenol brand in the Chicago area. After examining patients for the cause of death it was determine the capsules taken by those consumers were laced with cyanide. The next order from the crisis team was to warn the public by informing and cooperating with the media. To help communicate with the public Johnson & Johnson installed thirty-three phone lines and pre-taped statements were placed on special toll free telephone lines to expedite news gathering. The first article about the Tylenol crisis ran in the Chicago Tribune, supporting Johnson & Johnson during their investigation to find the perpetrator. Having the support of the Chicago Tribune can be lead back Johnson & Johnson having a great reputation amongst publics and the media and in this case the media aligned with the organization, because of the transparency displayed by the company.

Johnson & Johnson further identified and informed key publics on what happened and the initiatives taken by the organization to find the perpetrators. Fearn-Banks (2011) noted that, "All publics were notified and the crisis team kept in touch throughout." Concluding the investigation to find out who was responsible for the crisis, it was established that cyanide was not due to error by manufacturer, but tamper by consumer. Johnson & Johnson began constructing a plan that would prevent future contamination of products. They devised a plan called the triple-seal safety that would be applied to all bottles of Extra Strength Tylenol and

discontinued the former model of the brand. Next, the company gave away coupons for the new Tylenol product and set up toll-free lines where consumers could call and learn more information about the product and promotions. Finally according to Fearn-Banks (2011), Johnson & Johnson broadcast this information by satellite on twenty-nine sites where reporters were gathered, concluding the Tylenol crisis and return of sales for the Extra Strength Tylenol brand. Similar drug company's used the Tylenol case as a prodrome and began using the triple seal methods on similar products (Fearns-Bank, 2011, pp. 90-101).

Johnson & Johnson crisis illustrates how crisis communication was not necessary until a crisis with the possibility of causing harm to the general public occurred, instilling fear into the organization, causing them to react and strategize on how to handle future crisis. This case study further proves how an organization that is customer focused, are able to swiftly update publics and create a solution to the problem. Their reaction served to provide a strategy for other organizations to prepare in advance for future crisis.

As Harris, Hart, Hibbard, Jorgensen, and Wells noted "the Johnson & Johnson Tylenol crisis is an example of how an organization should communicate with the various publics during a crisis. The organization's leadership set the example from the beginning by making public safety the organizations number one concern. This is particularity important given the fact that Johnson & Johnson's main mission with Tylenol is to enhance the public's well-being or health" (2002).

Exxon Valdez

On March 23, 1989, Exxon Valdez ran aground off Alaska and dumped 250,000 barrels of oil into Prince William Sound, causing the waters to no longer be attractive and sea life to

perish. Exxon was regretful of the spill and their immediate effort was to swiftly clean up the oil spill and restore normalcy to area (Fearn-Banks, 2011). However, Public Relation experts criticize Exxon for further aggravating the damage to its public standing by failing to seize control of developments after the spill and establish itself as a company concerned about the problem it caused, according to reporter of the NYTIMES John Holusha, 1989. The overall response rate of Exxon was slow when it came to controlling the leakage of oil into the sea, infuriating fishermen and environmentalists. To handle the crisis Exxon's chairman, Lawrence G. Rawl, sent lower ranking executives to Alaska to handle the crisis, because he felt he was technologically obsolete and would "do nothing but get in the way" of clean-up efforts (Fearn-Banks, 2011). Furthermore, as pointed out by Holusha (1989), "this gave the impression that Exxon regarded the pollution problem as not important enough to involve top management."

Exxon set up a media center in Valdez, a remote town with limited facilities, equipment's, and accommodations to help communicate information to the media and publics. Four days after the spill the representative for the Valdez site Frank Igrossi, gave a press conference without being briefed by Public Relations Personnel, and was thrashed by reporters. What upset publics the most during the crisis is Ingrossi's refusal to verify the extent of the damage and what Exxon was doing to contain the spill. As a result, customers began canceling Exxon credit cards, the fishermen, environmentalists, and media became irate, and the media attacked more vociferously". Therefore, increasing the impression of a company that was not responding vigorously (Holusha, 1989).

After realizing the seriousness of the issue Exxon brought in George Mason who at the time was the Vice President of Bradley/Mcafee, Public Relations. He began delivering the overall recovery of Exxon by doing the following:

> Mason was asked to develop and implement strategies for three areas that he expected would be of future concern: tourism industry, animal rescue centers and the seafood industry. Several animal rescue centers were set up to help rescue some of the animals. Media tours were arranged and guidelines were established to guarantee the protection of animals. The strategy used to bring back tourism to Alaska was to create a campaign where travel writers would be flown to a part of Alaska where oil wasn't present, to witness the continued beauty of Alaska. Telephone hotlines were set up. News conferences were set up in influential cities like San Francisco, Los Angeles, San Francis, and Seattle. Finally, advertising and PR campaigns were organized by Exxon in conjunction with Mason's agency and McCan-Erickson of Seattle. The PR Campaign reached 50 million Americans, however the advertising campaign reached even more. As a result, tourism in Alaska increased by 5% more than the year before the oil spill (Fearn-Banks, 2011 pp. 104-106).

The case of Exxon serves as one of the worse handled crisis in the history of crisis management and as a model of what organizations should *not* do when handling a crisis. Unlike Johnson & Johnson, Exxon was not focused on their customers. Their response to the crisis appeared meaningless and angered publics due to their lack of concern for their mistakes. Several people were blamed for the oil spillage; however, Exxon as a whole lacked the initiative to take responsibility for the crisis and had weak leadership that did not understand the importance of having an actual presence during the crisis and the responsibility of the organization to keep publics informed.

Best Practices during a Crisis

After the case of Johnson & Johnson and Exxon crisis management practitioners began developing best practices that would help organizations develop crisis communication strategies that would prepare the organization for a crisis and when faced with a crisis, focus on maintaining an open line of communication with publics. The following best practices were developed in accordance with the perfections and inaccuracies of the Johnson & Johnson and Exxon cases. These exemplars will outline the traditional methods to handling and responding to

crisis. These practices were originally outline by Matthew Seeger (2006), however, many have been redefined and modified by scholars like Robert L. Heath and Shan R. Veil, with an addition of two best practices that are needed during the evaluation stage of a crisis.

Crisis communication needs to be an integral part of the crisis management plan in order to effectively communicate and warn publics on why a crisis is happening to the organization and how they can protect themselves from the crisis. When organizations fail to make crisis communication part of their overall communication strategy they risk the opportunity of negative publicity and severance of relationships with publics. Seeger (2006) says communication strategies are more effective during the planning phases of crisis, opposed to the actual event. The following best practices should be adhered to during the pre-crisis phase:

Pre-Crisis Communication	Letting people know that a crisis could occur, which responses are appropriate to that event, and that some entity cares for the well-being of the potentially affected publics (Heath, 2007).
Plan for a Prompt Response	Every member of the crisis communication team should be aware of his or her specific duties during a crisis. The crisis plan should include who, what, where, and when of the response to provide the organization with easy-to-follow guidelines during the initial confusion of the crisis (Veil & Husted, 2012)
Establish a Crisis Communication Network	The crisis communication network should include internal information sources and actors at all levels of the organization, outside agencies and the media. Further, establishing a network for which you can and should call on before the crisis is essential to administering an efficient and effective response during a crisis event (Veil & Husted, 2012).

When Experiencing a Crisis

When an organization is experiencing a crisis it is important for them to maintain communication and keep publics at the center of their attention before focusing on the organization. When organizations are actively involved in a crisis they should do the following:

Accept Uncertainty	When communicating with the media during a crisis, it brings about uncertainty within an organization and its publics. The organization should admit that all the facts aren't known at the time, and when they become available, further updates will be made (Seeger, 2006).
Form Partnership	The concerns of publics and stakeholders should be considered and taken into account and responded to by the appropriate crisis team member. Responding to concerns of stakeholders and publics makes the organization credibility rise, also forming relationship or partnerships with organizations and publics can expedite the recovery process (Veil & Husted, 2012).
Listen to Public Concerns	What may affect an organization during a crisis isn't always what affects publics. Listening to public concerns and addressing them should be done before a crisis, which helps build credibility in case a crisis happens an organization will still be favorable amongst publics after the crisis is over.
Honesty, Candor, and Openness	Organizations should exhibit honesty, candor, and openness. Facts will emerge and the harder the organization tries to hide them, the more explosive they are once they reach the surface (Heath, 2007).
Meet the Needs of the Media and Remain Accessible	The public typically learns about crisis through the media rather than the organization. The media is seen as unbiased and credible in the eye of the public gatekeepers who filter between what's legitimate and what is not. The organization should present accurate and full reports to the media, because if the media suspects false information, they'll expose the organization, which makes a crisis worse.
Communication with Compassion	Whether communicating with the general public, media, or other employers, designated spokesperson should demonstrate appropriate levels of compassion, concern and empathy

	(Seeker, 2006). This is necessary in order for publics to understand you care about how the crisis has affected them and serve as the first phase of recovery for the organization.
Self-Efficacy	These types of messages give individuals ways to protect themselves against the crisis, rather it be physical, emotional or psychological. This allows for publics to feel the organization knows there is a crisis and shows them how they can protect themselves; therefore the organization's image usually is not tarnished after a crisis has run its course.
Be Committed and Deliver on Time	Don't give reporters an extra incentive to doubt your version of the crisis and seek a better version of the truth elsewhere (Heath, 2007).

Recovery Process

After a crisis has ran its course it is not over. Organizations must go back and visit how the crisis was mitigated and determine if anything could have been done better to communicate better with publics. They then need to take the lessons learned and incorporate them into the overall crisis communication strategy, therefore preventing the same error from being made in a similar crisis. After organizations have returned to normal or a new norm they should do the following:

Post Crisis Communication	Offers organizations the opportunity to get out key messages to the media while having their attention (Heath, 2007).
Evaluation of Overall Crisis Response Strategy	If an organization manages to survive a crisis, it is important to evaluate what went right or wrong and what could be done to better serve or provide information to the publics. Further, what could have been done differently so that the crisis of this magnitude is averted?
Provide Follow-Up	Provide follow up information to publics and change old business model to reflect new changes learned from the crisis.

These practices can be best associated and explained by the Situation Crisis Communication Theory (SCCT). Coombs (2007) says that SCCT provides an evidence-based

framework for understanding how to maximize the reputational protection afforded by post-crisis communication. SCCT matches the level of the crisis response with to the level of crisis responsibility afforded by the crisis. It is designed to provide a set of guidelines that can be used for crisis response strategies to protect the reputation of the organization (Coombs, 2007).

Coombs (2011) suggests that there are two types of reputations, one for the perspective of the organization and the other from the perspective of the stakeholder. "From the perspective of the organization, reputation is an intangible asset that allows the company to better manage the expectations and needs of its various stakeholders; however, from the perspective of the stakeholder reputation is the intellectual, emotional and behavioral response as to whether or not the communications and actions of an organization resonate with their needs and interest. Therefore, providing instructing information, that is, what publics need to know and do to protect them from the crisis, is necessary before addressing reputational concerns of the organization (Coombs & Holladay, 2002).

After the organization has provided publics with information on how they can protect themselves from the crisis, organizations must assess its reputation and determine if the organization is at fault. If the organization is deemed responsible, their reputation will suffer, therefore causing publics to cut ties with the organization and potentially create a negative word of mouth (Coombs, 2007). Three factors that help determine the level of threat the organization faces are initial crisis responsibility, crisis history, and prior relational reputation. Initial crisis responsibility helps determine who is responsible for the crisis, rather it be the organization or some outside agent that caused the crisis; crisis history is whether the organization has had similar crisis in the past; prior reputation is rather the organization has a history of treating stakeholders badly. Once the organization has assessed the impact the crisis will have on both

stakeholders and the organization it is important to implement crisis response strategies that will communicate the crisis to stakeholders.

Crisis Response Strategies

When there is a crisis, there must be communication with the news media, social media, publics, internal publics, external publics, and lawyers (Fearns-Banks, 2011). Further, practitioners should be responding the first hour after the crisis occurs (Coombs, 2011). Therefore, the organization needs to tell its side of the story, which according to Coombs (2011) is key point's management wants to convey about the crisis to its stakeholders. A combination of traditional news media, online news media, and social media should be used to effectively and efficiently communicate the crisis to publics and what the organization is doing to correct the crisis. Fearn-Banks (2011) says both traditional media and social media should be contacted at the same time and immediately, because if accurate data isn't disseminated, inaccurate data is.

When communicating crises to publics it is important to have one voice speaking on the behalf of the organization. Speaking in one voice for the organization can be seen through multiple lenses. For example Hutchens PR claims that companies should identify one central spokesperson at the highest level possible, and make sure the individual has the knowledge, sensitivity, interpersonal skills, authority and public demeanor to speak on the behalf of your organization. When multiple spokespersons are appointed to speak on the behalf of an organization during a crisis it is important for public relations staff to take notes of what was said by one speaker to covey a consistent message. After establishing the spokesperson for the crisis it is important to communicate the same message across all mediums.

Majority of publics still consume news from traditional media sources, making television and radio the most effective methods used to reach publics. The news media are drawn to crises and are a useful to reach a wide array of publics quickly (Fearn-Banks, 2011). Usually it is difficult for organizations to get media outlets to use a simple press release from the organization, however Fearn-Banks (2011) and the Institute of Public Relations agree, it will be the news media who will lead the initial charge to fill information, considering they are gatekeepers and represent the public's interest. It is in the organizations best interest to provide the news media with accurate information; otherwise they risk the potential of inaccurate information being spread about the crisis, causing the crisis to worsen. If the organization has provided inaccurate information, it is important to regain control of the situation as soon as possible (Fearn-Banks, 2011).

Relying specifically on news media coverage is not enough to communicate the crisis to publics, however web sites, intranet sites and mass communication systems adds to the news media coverage and help provide a swift response (Coombs, 2007). When organizations experience crises it is important that internal publics (employees, management, and owners) receive communication about the crisis and how they can either protect themselves or how they can help the organization navigate the crises and return to normal. One medium used to communicate information to internal publics is by using the company's intranet. An intranet is a private network, operated by a large organization, which uses internet technologies, but is insulated from the global internet (Schofield, 2010). Intranet sites limit access, typically to employees; however customers and suppliers may also have access, providing direct access to information for stakeholders (Coombs, 2011). According to Holtz (2004) if you have an intranet,

you can set up crisis templates that include the kind of information that never changes, therefore allowing the rest of the information to be filled in whenever the crisis emerges.

Intranets are primarily used for communicating crises to internal members of the organization; however customers, communities and governments, suppliers and creditors all have an interest in the organization. This group of people is referred to as external stakeholders, which are any person, group or organization that has an interest in the activities and affairs of a company (Kokemuller, 2014). One of the first places people go to look for information is a company's website. The everyday website of an organization may not be the best option to showcase the crisis, because during normal operations websites promote a company or organization and its products or services (Bell). However, according to Bell, during a crisis, stakeholders want, need and expect very different, specific and consistent factual information from a trusted source, which is when a dark web site becomes valuable.

The Center for Infectious Disease Research and Policy (CIDRP) defines a dark web site as a pre-made, non-visible web site that is activated when a crisis or emergency occurs. When a crisis occurs, due to the fast pace and demand for information, there is no time to construct a new site from scratch. But, having a prebuilt site that can simply be turned on when needed is more effective, because basic information is already uploaded, therefore allowing the organization to upload information about the crisis to the website. According to Luttrell (2014) the website can serve two purposes: first, the website can minimize the conversation happening on social sites; second, the website illustrates that the company is proactive in resolving the issue at hand. Having a website that provides continuous updated information to publics, shows the organization is interested in maintaining a transparent relationship, which could be a positive step to recovering from the crisis.

Social Media Crisis Response Strategy

The Johnson & Johnson and Exxon Valdez case studies illustrate an idea that has become more prevalent with the expansion of 24 hour electronic media. The media will often be the first on the scene, thus have information about the crisis before the organization does (Berge, 1990).When Johnson & Johnson and Exxon experienced their crises during the 1980's they used television, radio, Internet, and newspapers to effectively communicate messages to publics, often falling under the traditional methods of communication. These methods of communication worked for these organizations, because at the time they were popular ways consumers sought information. However, in the 21st century, contemporary methods of communication make it harder for organizations to focus on one specific medium to communicate with stakeholders. In order for organizations to be successful during a crisis they must use a combination of traditional and contemporary mediums of communication to effectively reach all publics. Luttrell (2014) notes, despite having traditional crisis plans in place, companies find that they are not prepared to manage a crisis on the social sphere.

Social media provides a platform where organizations can share information, build trust, and credibility, therefore leading to a more transparent relationship between the organization and publics. During a crisis social media serves as a medium where the organization can control the information that publics see and provides an opportunity to reach out and tell their side of the story. Further, it allows the opportunity for the organization to receive feedback from publics and properly observe their concerns by letting publics know what the organization is doing to handle the crisis. When the organizations combine traditional media communication and social media communication it results in reaching a greater audience affected by the crisis (Lead & Lewis.

2012). Below is a chart created by Laad & Lewis (2012) that further illustrates the benefits of using both traditional media and social media during a crisis.

Social Media Communications	**Traditional Media Communications**
Internet and mobile-based means of communication (social networks, blogs, etc.)	Traditional means of communication (television, radio, newspapers, magazines)
Engaging people/audience	Informing people/audience
Unstructured sharing of information	Structure sharing of information
Two-way communication (Dialogue)	One-way communication (Monologue)
Quick and instant information dissemination	Bound to fixed schedule, press deadlines
Talking to Consumers/Customers	Talking at Customers/Consumers
Public/Audience exercise control on the flow of information	Government/Businesses/organizations exercise control on the flow of information
Decentralized information distribution process	Centralized information distribution process
Consumer sponsored communication	Organization sponsored communication
Fuelled by internet research, peers and friends options, preferences and recommendations	Fuelled by organizations' advertising/marketing campaigns
Trustworthy and transparent	Speculates and lacks transparency

Foster Citizen Journalism	No public involvement
Potential dangerous as it can easily lead to rumors/gossip monitoring	"Gatekeepers" prohibit irrelevant and false information
Practical, easy and inexpensive	Unpractical, complicated and expensive

Chart from (Laad & Lewis, 2012 pp.15)

Domino's Pizza

To further illustrate the usage of social media and its effectiveness when navigating a crisis via social sphere we will examine the 2009 Domino's Pizza hoax by using the five stages of crisis management in the digital age by Palubicki (2013).

On Sunday April 12, 2009 two Domino's employees from North Carolina uploaded a video to YouTube. The video consisted of an employee putting cheese up his nose and putting it on sandwiches that would be delivered to customers, all while another employee provided commentary. The two employees said they never planned to deliver the sandwiches and it the video was supposed to be a prank. The two employees were arrested and charged with criminal acts and immediately fired from Domino's. This case can be seen as one of the most effective methods of using social media to navigate a crisis on the social sphere. Palubicki (2013) offers five stages of the crisis management cycle in the digital age:

1. Prepare in advance. Thinking of what could happen before it does and having a plan on how to deal with the issue is a must. Domino's at the time of the crisis did not have a social media presence; however the organization had developed a social media plan that would have been implemented one week after the crisis if it had not occurred. Although they did not have a presence the organization was still prepared to handle the crisis by enacting the plan earlier than expected.
2. Identify the origin. Locating the point of origin for the crisis and determining where majority of the information fueling the crisis is coming from is important. Domino's did

not have to search far for the point of origin, considering the video was released on YouTube. However, majority of the conversation began taking place on Twitter, where Domino's had no presence yet.

3. Assess the Impact. This determines how the organization has been immediately impacted by the crisis. The Domino's crisis took off quickly and immediately impacted the organization, considering that information can spread on the social sphere within seconds. Domino's was impacted in the following ways: the video originally uploaded by the Domino's employees reached 3 million hits the day after it was uploaded, according to the NYTIMES.COM; customers began talking about the hoax on Twitter where Domino's did not have a presence; 65 percent of customers who visited Dominos Pizza said they would not visit after seeing the video, according to the Wall Street Journal, HCD research, 2009; the hoax was found in 5 of the top 12 search results presented by Google to users; after the original video was deleted a second copy appeared generating 345,000 views.
4. Mitigate the Crisis. This section details what the organization did to lessen the force of the crisis. Coombs (2007) says, crisis managers must be where the action is and respond in the social media where the crisis originated. First, Domino's realized that the crisis was erupting in the social sphere and the viral video reached one million hits, they immediately launched a Twitter account to inform visitors the hoax was an isolated event and the company was doing everything it could to correct the problem. Next, Domino's posted an official apology on the company's website and asked their loyal fans to repost the link. Finally, Domino's released an official statement on YouTube, the same medium the crisis erupted on explaining what happened, told customers the incident would not happen again and presented the actions being taken to fix the problem.
5. Learn from Your Experience: Crisis present a unique learning opportunity where organizations can gain valuable insight. After the crisis is over and the organization has returned back to normal or a new norm has been created organizations should look at communication strategies and evaluate what worked and what did not. Some of the valuable takeaways from Domino's crisis are:

    - Domino's launched a campaign informing customers the organization wanted to hear from them more regularly.
    - Domino's actively participates in social media from handling customer complaints or talking about its promotions.
    - Domino's teaches its franchise owners that crisis management begins in the preparation phase.

Domino's pizza crisis serves as a benchmark for how organizations can effectively use social media to conduct environmental scanning to see what is being said about the organization and prepare in advance if a crisis is brewing. Building a brand with a loyal customer base as Dominos did, ensures that while navigating a crisis you'll be able to call upon customers to help

defeat the crisis. Overall, having a customer centered focus is paramount as it could depend on the survival of the organization.

METHODOLOGY

Many case studies have been published by organizations detailing the importance of organizations having a crisis management plan that is continuously updated; however there is limited research on the communication strategies used during a crisis to effectively prepare publics for a crisis. For this study Target Corporation was chosen, because it was the first organization to experience the data breach and the first organization to serve as a prodrome for other organizations that will experience a data breach following there's. To develop the context of this study, information was obtained from Target Corporate website. Further, news articles were obtained from various news outlets to develop a full description of the crisis. This study aims to answer the research question of does using benchmark crises and best practices aid in helping crisis leaders develop a crisis response strategy that will result in the recovery of the organization with minimal damage to its reputation? In order to draw conclusions from this information a combination of best practices is used.

Target Corporation Data Breach

On November 27, 2013 on Black Friday the busiest holiday shopping season of the years, hackers infiltrated Target Corporation network causing a major data breach. The data breach is suspected to have happened November 27-December 18, 2013. On the evening of December 12, 2013, Target was notified by the Justice Department of suspicious activity involving payment cards used at Target stores. Target claims they launched an immediate investigation meeting with members of the Justice Department and Secret Service, immediately following with an

investigation from a team of outside experts. As the investigation unfolded Target concluded forty million customer credit and debit card information was compromised. Stolen debit and credit card information included customer names, credit and debit card numbers, card expiration date and CVV (card verification value). Further, seventy million additional customers were affected having their person information stolen from Targets servers, which included customer names, mailing addresses, phone numbers, and email addresses. However, Target vows the information stolen was "partial in nature", therefore serving of little use to hackers.

Between February-March 2014 Target was invited to a congressional hearing to talk about why the data breach occurred and what was being done to solve the problem. During the Congressional Hearing before the Senate Committee of Commerce, Science & Transportation, Executive Vice President and Chief Financial Officer of Target John Mulligan claimed, "We believe the intruders entered our system on November 12. We know that the intruder's activity was detected by our computer systems, logged and surfaced on the SOC and evaluated by our security professionals." Further he claims hackers obtained an HVAC Vendor's Credentials to the outermost portion of the network. The malware appears was designed to capture payment card data for magnetic strip credit and debit cards. On December 15, 2013, target removed the malware from their point-of-sale network and two days following informed payment processors and card networks about the breach, preparing to officially announce the data breach to the public.

On December 19, 2013, Target announced to the general public that 40 million credit and debit cards were compromised. Further they communicated that additional 70 million customer personal information was compromised. As of January 10, 2014, a total of 110 million customer's information was compromised from the data breach. Target used a multitude of

channels to convey message to customers including a mass-scale public announcement, email, prominent notice on their website, and social media.

Besides customers being affected by the data breach other individuals and organizations. For example, former President and CEO Gregg Steinhafel resigned his position as Chairman of the Target Board of Directors, however the Board of Directors asked him to continue serving in an advisory capacity. He believed himself to be responsible for the data breach and believed Target would emerge a better company. Next, according to Matthew Rocco from the Fox Business, "credit unions and banks estimate the data breach cost them 200 million dollars." These figures are an estimate of how much it costs banks and credit unions to replace customer's stolen credit cards, money in which they believe Target has no intentions on replacing. Finally, organizations that rely on using customer's credit and debit card numbers to pay for monthly subscriptions struggled with keeping information up-to-date. For example, in an interview with Amy Kiley, Rocky Arbitell, claims he hates the sounds of gym's scanner rejecting a membership card. Unfortunately it is what greets about thirty percent of people coming to work out at his Orlando, Florida business, The Gym Downtown." Further, he claims that since January 2014 his company has lost approximately $57,000.

Target claims its response to the breach has been to inform the public how they can best protect themselves against the ongoing cyber threat. To protect publics and the organization Target has implemented the following strategies, according to Vice President and Chief Financial Officer John Mulligan of Target during the Congressional Hearing before the Senate Committee on Commerce, Science, & Transportation:

- Segmentation: Target is increasing the segmentation and separation of key portions of their network by enhancing the protection provided by the firewalls they have in place to limit unauthorized traffic.

- Whitelisting: Target has accelerated the installation of whitelisting solutions to its registers. Whitelisting protects guests by detecting malicious applications and stopping them from running on the registers and gives Target another tool to prevent malware from taking root and spreading throughout the environment.
- Authentication: Target is strengthening its network by installing two-factor authentication for entry into the system.
- Target is making sure the right people, with the right experience, are in the right place. They are taking a hard look at their organization, with the intention of bolstering their information security structure and practices.
- Target became the first retailer to join the Financial Services Information Sharing an Analysis Center (FS-ISAC), an initiative developed by the financial services industry to help facilitate the detection, prevention, and response to cyber-attacks and fraud activity.
- Target is accelerating its 100 million dollar investment in the adoption of chip technology to enhance consumer protection.
- They continue to reissue new Target credit or debit cards immediately to any guest who requests one.
- They are offering one year free credit monitoring and identity theft protection to anyone who has ever shopped at any U.S. Target stores.
- Guests have zero liability for fraudulent charges on their cards arising from the incident.

Target claims that it has learned from its mistakes and wants to be the premier retailer to protect its customers by ensuring its organization is equipped with the best software to prevent another data breach.

Analysis

Using the best practices model to assess the organization's purpose provides a framework for highlighting successes and pinpointing failures. By breaking the response down, best practices analysis helps practitioners and crisis communicators learn the right lesson from past crisis responses. Target Corporation crisis response is outlined here according to the best practices framework.

Identify the origin and Planning for a prompt response

- Target claimed on December 12, 2013, the U.S. Justice Department notified the retailer about the data breach and six days following the notification they notified the public. In this case it appears that Target was unaware of the data breach until it received

notification from the U.S. Justice Department, however an investigation was conducted by Bloomberg Businessweek resulting in a different outcome. In the report it was concluded that Target was prepared for the data breach. Six months before the data breach Target installed a $1.6 million malware detection tool made by the computer security firm FireEye, who also makes similar security tools for the CIA and Pentagon. FireEye works by creating a parallel computer network on virtual machines. Before data from the Internet reach Target, they pass through FireEye's technology, which spots attack before it occurs and warns Target. Further, Target has a security team located in Bangalore that monitors there security systems and if an attack were detected it would be reported to the security office in Minneapolis would be notified.

- During the time in which hackers were uploading exfiltration malware which was used to move stolen credit and debit card numbers off targets servers onto computers in Russia, FireEye detected the attack. Bangalore reported the attack to the security team in Minneapolis, however nothing happened on Targets behalf. In testimony before Congress, said after the Justice Department informed them of what happened their personal investigators went back to see what happened. However, Target failed to reveal that it found FireEye's alerts from November 30. It is possible that if Target would have acknowledged the initial warning from FireEye the malware installed by hackers could have been eliminated before transmitting stolen credit and debit card information of Target's networks. Therefore, it appears Target is responsible for the data breach, because the company had the correct systems in place; however they ignored valid warnings, resulting in 40 million customers having their credit and debit card information stolen and 70 million customers personal information compromised.

- When Target finally acknowledged the data breach after being notified by the Justice Department on December 12, 2014, they immediately notified payment processors, card networks and the general public about the data breach, notifying them they were aware of the event and were doing everything to investigate what happened and catch the perpetrators. Ultimately, Target waited days after being notified about the data breach to announce it to the public.

Assess the impact

- Target experienced a forty-six percent drop in profit in the fourth quarter of 2013 compared with the year before the data breach. Also, Target is suspected to spend $100 million in replacing their credit card payment terminals. According to statistics from analytics firm Crimson Hexagon, "from December 18-19, almost three weeks after the hack, more than 587,000 tweets relevant to Target's credit card breach were sent, a rate of about 12,000 per hour. Twitter was mentioned more than 48,000 times and the hashtag #target had more than 31,000 mentions December 18-19 and #databreach had more than 5,200 mentions.

Establish a crisis communication network

- The data breach experienced by Target was unexpected, however the organization moved swiftly with identifying the key members of the crisis communication network. Former CEO Gregg Steinhafel served as the spokesperson for the organization until he resigned and was replaced by John Mulligan.
- Target set up a crisis network where customers could either call a hotline or visit the company's website to learn more information about the data breach and have questions or concerns addressed.

- Outside the organization Target gave information to credit report agencies where customers could receive credit report monitoring and request a credit report. Further, while the organization did not communicate with government officials before the crisis, during the crisis John Mulligan attended congressional hearings informing Congress of what happened and what was being done to stop the data breach. By Target creating a crisis network it has provided the necessary information for employees, government agencies, and customers to protect themselves from the ongoing data breach.

Accept Uncertainty

- Target did not address acknowledge uncertainty of the crisis. The organization primarily focused on what it did know-40 million customers credit and debit card information was stolen by hackers, but did not address the fact of what they did not know-other customer information besides credit and debit card information could be compromised. Furthermore, the organization did not make mention to customers that Target's data breach could set off a chain reaction with other retailers so retailers and customers should prepare to combat future attacks. During the data breach target did not seem to fear the unknown, but continuously expressed what the organization was doing to make sure the issue was resolved. They continuously updated their website, providing customers with updates every time they found something or implemented a new strategy or technology that would resolve the crisis. Also, Target stated that they couldn't confirm if social security cards were missing, but told customers not to be worried, because the data stolen was partial in nature.

Form Partnership

- Target did work with partners during the data breach. For example in Target's initial statement they announced: "We are partnering with a third-party forensics firm to conduct a thorough investigation of the incident and to examine additional measures we can take that would be designed to help prevent incidents of this kind in the future."
- Target also partnered with the credit reporting agencies to provide customers with free one year credit report monitoring and to dispel any charges to the customer as a result of the breach. In addition to partnering with credit reporting agencies Target partnered with the Secret Service who usually handles data breach investigations. Finally, Target became the first retailer to join the Financial Services Information Sharing and Analysis Center (FS-ISAC), which is an initiative developed by the financial service industry to help facilitate detection, prevention, and response to cyber-attacks and fraud activity.

Listen to public concerns

- Target acknowledged public concern by continuously keeping them up-to-date on the breach and what they could expect the organization to do in the future. Target also announced that it was adding more workers to field calls to handle the influx of calls about the breach. Finally during the holiday season 2013 Target offered customers ten percent off of majority of the items in the store, the same discount given to its employees.
- Target also took the time out to acknowledge customers questions and concerns via social media. Each customer complaint at the beginning of the crisis received a response, regardless if the response was generic and the same message tailored to one customer was used on the next. However, toward the end of the crisis January 10, 2014, as customers continued to express outrage and frustration Target stop responding to these customers. When organizations experience a crisis publics are going to be outraged, especially when

confidential information that is trusted with the organization is compromised and sold online on the black market. Customers have a right to feel entitled to a response, especially if it is the organization at fault for the crisis, but fault is still to be determined as the Secret Service and Congressional Committee completes their investigation.

Communicate with honesty, candor, and openness

- Target was open and honest about its actions during the data breach and kept customers informed on what was happened for the most part. However, as noted in the Bloomberg Businessweek report, Target was accused of ignoring warning signs that should have prevented the data breach in its entirety. However, Target never openly responded to this accusation by saying if the report was true or false, but responded with this statement from Target Chairman, President, and Chief Executive Officer Gregg Steinhafel in an email: "Target was certified as meeting the standard for the payment card industry (PCI) in September 2013. Nonetheless, we suffered a data breach. As a result, we are conducting an end-to-end review of our people, processes and technology to understand our opportunities to improve data security and are committed to learning from this experience. While we are still in the midst of an ongoing investigation, we have already taken significant steps, including beginning the overhaul of our information security structure and the acceleration of our transition to chip-enabled cards. However, as the investigation is not complete, we do not believe it is constructive to engage in speculation without the benefit of the final analysis."
- By target not responding to this statement it seems as if the organization is either hiding something from the public or they don't want to misspeak, considering they could criminalize themselves if the organization speaks out of turn. Furthermore, it seems

Target is pointing out that they were a victim of the crisis as well, considering they were certified for the PCI.

Meet the meet the needs of the media and remain accessible

- Target met the needs of the media throughout the crisis by issuing multiple press releases and constantly providing updates about the crisis on their corporate page.

Communicate compassion

- Target communicating with compassion is closely tied with listening to public concerns. By Target addressing customer via social media it provided them the opportunity to make customers aware that it was sorry for them having to experience the data breach and Target would be with them every step of the way. Customers feared their information would be stolen and used by hackers, however Target made people feel at ease when it responded by telling customers any charges that occurred due to the data breach would be handled by Target.

Provide suggestions for self-efficacy

- During the crisis Target continuously repeated in multiple forms and on multiple channels how customers could protect themselves from the crisis. For example they recommended that customers remain vigilant for incidents of fraud, regularly review account statements and monitor free credit reports. Further, they provided customers with contact information of the Federal Trade Commission (FTC) or law enforcement agencies in case they needed to report an incident.

Continuously update and evaluate crisis plans and learn from your experience

- Considering that Target was the first company to be affected by data breach they set an example for other organizations to follow pending they encounter a data breach. Target

has begun taking a look at itself internally to ensure the right people, with the right experience, are in the right place. It has strengthen its anti-virus tools, accelerated the plans in adopting chip technology and installing chip enabled payment devices in Target Stores, and they plan to issue chip embedded Target REDcards by early 2015. Target understands that if future data breaches are to be prevented it cannot be the sole organization acting on this initiative, but must include all organizations to keep something like this from happening again. Target continues to update customers on the investigation of the data breach as it becomes available.

FINDINGS AND LESSON LEARNED

The major flaw with Target's data breach is they waited days after being told about the breach to announce it to customers. However, Target made positive contributions to the data breach they experienced during the Black Friday holiday season in 2013. Although Target is still being investigated by secret service and the congressional committee and have not announced if the accusations of Bloomberg Businessweek are correct, it has come forth with providing customers with the most accurate information detailing the data breach. During the breach Target experienced backlash on the social sphere from concerned customers, however they continued to address customers and share information about the crisis and what was being done to handle the crisis via social media. The company was quick to establish a crisis communication network, therefore establishing the leadership that would be responsible for handling the crisis. However, the organization did not accept uncertainty making it seem as if Target did not care about the unknown. Target also established partnerships with third-party organizations to help investigate the crisis and provide customers with information that could be used to survive the crisis. The overall communication of Target during the crisis was with compassion and honesty and kept the

public at first thought. Finally, the organization established next steps on how it would become the premier retailer in preventing further data breaches.

By evaluating Target's response to the data breach four lessons can be learned, which were outlined by Freelance Journalist Natalie Burg (2014) in Forbes Magazine:

1. Communicate crisis to publics: When an organization experiences a crisis it should be the first person to broadcast the crisis to customers regardless of what information is not known, opposed to customers hearing it from an outside organization. Target knew about the data breach a week before it sent an official notice to customers, however probably would not have published the information when it did if it would not have been for the website Krebs on Security publishing the first article about the breach.
2. Be ready to respond to your customers: When target released the official statement about the data breach it did not have the staff to deal with the influx of inquires that came from the public. For example, phone lines were jammed and social media channels were flooded with comments from angry customers. When an organization experiences a crisis it should know in advance that additional staff will be needed to handle customers concerns, otherwise not addressing these concerns could result in the loss of trust from the organization to the customer.
3. Updated Security Technology: The United States is one of the last countries to use the magnetic strip cards instead of the chip enabled cards. If data breaches are to stop in the U.S. then organizations need to push for updated technology that prevent such acts from occurring.
4. Rebuild Trust: Target has launched a fierce public relations campaign to show customers that the organization can be transparent and forthcoming with information. In order for target to recover it needs to continue to put customers first and stick to the promises made during the initial crisis response.

These lessons can, not only be applied to Target's response to the data breach of 2013, but also to the expanding data breaches faced by organizations each day. Using best practices to evaluate the response of an organization during a crisis allows for a lesson to be learned and serve as a benchmark for future cases.

CONCLUSION AND FUTURE WORK

With uncertainty lingering on rather Target will be considered responsibly for the data breach, because they ignored warning signs that could have prevented the breach or if malware

detection tools used by Target were tricked by hacker's disguises, all will be determined pending the results of the investigation.

There are many aspects of the study that could have made the results more comprehensive. The time in which Target's data breach occurred and the results of data breaches experienced by other organizations is scattered, therefore leaving Target as the only organization have fully combat the crisis and proceed to recovery and building trust with customers. Analyzing more than one crisis would have allowed an analysis detailing if Target is considered a prodrome for other organizations and if not conduct compare and contrast the similarities and differences of each organization's crisis response strategy.

The second limitation experienced was choosing the proper methodology for the literature that would best reflect the research results. Choosing another method would require further information, which hasn't yet been released due to pending investigation results. This is why the best practices approach was chosen, because it enables the reader to view previous benchmark crises with similarities and use old best practices and contemporary practices to evaluate the response of the organization.

Despite the few limitations, there are solutions to allow any further research to delve more into the topic of study. First, after the investigation of Target is completed it will be revealed who is responsible for the data breach. Knowing who responsible will determine the fate of the organization. If the organization is deemed at fault further analysis into the response strategies will be warranted, considering the organization will be facing the crisis in the court of public opinion. Second evaluating multiple crises will determine if Target's recommendations were considered by other organizations and if not an analysis of what other retailers did different to handle the crisis. This research will serve as benchmarks to handling future crises dealing with

data breaches and cyber-crime. I believe using the best practice approach in my research allowed me to conduct a strong study on the greatest data breach of the twenty-first century.

References

Banks, K. (2011). *Student workbook to accompany Crisis communications : A casebook approach, Fourth Edition.* London: Routledge.

Banks, K. (2011). "Textbook" Crises. In *Student workbook to accompany Crisis communications : A casebook approach, Fourth Edition* (pp. 90-106). London: Routledge. Coombs, T. (2011, January 6). Crisis Management and Communications - Institute for Public Relations. Retrieved December 13, 2014, from http://www.instituteforpr.org/crisis-management-and-communications/

Bell, S. (n.d.). Eric Mower Associates PR. Retrieved December 14, 2014, from http://www.mowerpr.com/reputation-management/our-experience/dark-websites-for-crisis-response/

Berge, T. (1990). The First 24-Hours. Cambridge, MA: Basil Blackwell, Inc.

Burg, N. (2014, January 7). Five Lessons For Every Business From Target's Data Breach. Retrieved December 14, 2014, from http://www.forbes.com/sites/sungardas/2014/01/17/five-lessons-for-every-business-from-targets-data-breach/

Coombs, W. T. (2007). Protecting organization reputations during a crisis: The development and application of situational crisis communication theory. *Corporate Reputation Review, 10*(3), 163-176. doi:http://dx.doi.org/10.1057/palgrave.crr.1550049

Coombs, T. (2011, January 6). Crisis Management and Communications - Institute for Public Relations. Retrieved December 14, 2014, from http://www.instituteforpr.org/crisis-management-and-communications/

Coombs, W. (2012). *Ongoing crisis communication: Planning, managing, and responding* (3rd ed.). Thousand Oaks, Calif.: SAGE.

Coombs, W. T., & Holladay, S. J. (2002). Helping crisis managers protect reputational assets. *Management Communication Quarterly : McQ, 16*(2), 165-186. Retrieved from http://ezproxy.emich.edu/login?url=http://search.proquest.com/docview/216315539?accountid=10650

Crisis Communication Plan - Dominican College. (2007, February 9). Retrieved December 14, 2014, from http://www.dc.edu/people/390-2/public-relations/crisis-communication-plan/

Crisis Communications Tips. (n.d.). Retrieved December 14, 2014, from http://hutchenspr.com/resources/crisis-communications-tips/

Dark site stores emergency communications until crisis occurs. (n.d.). Retrieved December 14, 2014, from http://www.cidrap.umn.edu/practice/dark-site-stores-emergency-communications-until-crisis-occurs-ca

Harris, V., Hart, D., Hibbard, B., Jurgensen, J., & Wells, J. (2002, January 1). Crisis Communication Strategies. Retrieved from http://www.ou.edu/deptcomm/dodjcc/groups/02C2/team members.htm

Heath, R. L. (2007). Best practices in crisis communication: Evolution of practice through research. *Journal of Applied Communication Research, 34*(3), 245-248. Retrieved from http://ezproxy.emich.edu/login?url=http://search.proquest.com/docview/621390648?accountid=10650

Holtz, S. (2004). Communicating Bad News. In *Corporate conversations: A guide to crafting affective and appropriate internal communications*. New York: Amacom.

Holusha, J. (1989, April 20). Exxon's Public-Relations Problem. Retrieved December 14, 2014, from http://www.nytimes.com/1989/04/21/business/exxon-s-public-relations-problem.html

Hutchens PR. http://hutchenspr.com/resources/crisis-communications-tips/

Kazlowski, C. (2010, January 1). Crisis Management. Retrieved December 13, 2014, from https://www.rqa-inc.com/newsletters/Catlin_US_U0110.pdf

Kokemuller, N. (n.d.). Who are the External Stakeholders of a Company? Retrieved December 14, 2014, from http://smallbusiness.chron.com/external-stakeholders-company-64041.html

Laad, G., & Lewis, G. (2012). Role of social media in crisis communication [White paper]. Retrieved December 14, 2014, from Gerald Lewis & Associates: http://www.geraldlewis.com/publications/Role_of_Social_Media_in_Crisis_Communication_Jan_2012_Gitanjali_Laad.pdf

Lando, A. L. (2014). The critical role of crisis communication plan in corporations' crises preparedness and management. *Global Media Journal, 7*(1), 5-19. Retrieved from http://ezproxy.emich.edu/login?url=http://search.proquest.com/docview/1543483211?accountid=1065

Lockwood, N. (2005). *Crisis management in today's business environment: Hr's strategic role.* Alexandria, VA: Society for Human Resource.

Luttrell, R. (2014). *Social media: How to engage, share, and connect*. Rowman & Littlefield.

NyBlom, S. E., Reid, J., Coy, W. J., & Walter, F. (2003). Understanding crisis management. *Professional Safety, 48*(3), 18-25. Retrieved from http://ezproxy.emich.edu/login?url=http://search.proquest.com/docview/200304480?accountid=10650

Palubicki, K. (2014, June 14). Friday Five: Crisis Management in a Digital Age. Retrieved December 14, 2014, from http://www.edelmandigital.com/2013/06/14/friday-five-crisis-management-in-a-digital-age/

Seeger, M. W. (2006). Best practices in crisis communication: An expert panel process. *Journal of Applied Communication Research, 34*(3), 232-244. doi:http://dx.doi.org/10.1080/00909880600769944

Veil, S. R., & Husted, R. A. (2012). Best practices as an assessment for crisis communication. *Journal of Communication Management, 16*(2), 131-145. doi:http://dx.doi.org/10.1108/13632541211217560