

HACKING A REPUTATION:
CRISIS COMMUNICATION AND THE ASHLEY MADISON DATA BREACH

by

Katherine Owczar

Bachelor of Arts (Honours), Media, Information & Technoculture

University of Western Ontario, London, Ontario, Canada, 2018

A Major Research Paper

Presented to Ryerson University

in partial fulfillment of the requirements for the degree of

Master of Professional Communication

in the Faculty of Communication and Design

Toronto, Ontario, Canada, 2020

© Katherine Owczar, 2020

AUTHOR'S DECLARATION FOR ELECTRONIC SUBMISSION OF A MRP

I hereby declare that I am the sole author of this MRP. This is a true copy of the MRP, including any required final revisions.

I authorize Ryerson University to lend this MRP to other institutions or individuals for the purpose of scholarly research.

I further authorize Ryerson University to reproduce this MRP by photocopying or by other means, in total or in part, at the request of other institutions or individuals for the purpose of scholarly research.

I understand that my MRP may be made electronically available to the public.

Table of Contents

1. Introduction.....	1
Background of the Crisis.....	3
2. Literature Review.....	6
3. Research Questions.....	19
4. Method of Analysis.....	20
5. Findings	23
6. Discussion.....	44
7. Conclusion.....	47
8. References.....	51

Introduction

At a time where online activists are targeting and obtaining the intellectual property of companies on a regular basis, how should a company communicate and mitigate the data breach to ensure that its valued customers feel protected, or in the best case scenario, prevent it altogether? The adoption and implementation of a sound crisis communication and management strategy is thus a fundamental operative for the success of any organization. Organizational crises can fundamentally disrupt and harm companies, organizations and individuals alike; they are characterized as “non-routine, severe event[s] that [can] destroy [its] reputation or operations” (Koerber, 2017). When a crisis arises for an organization, it is imperative that they have a strong sense of clarity regarding the issue at hand – specifically, they must understand the context and “background narrative that gives interpretative shape to [its] foreground issues” (Arnett, Deiuliis, Corr, 2017). Perhaps most emblematic of these background narratives is the circulation of competing information and perspectives, by both social media and traditional news sources. With the rise of social media and the 24/7 news cycle, a new sense of power and inflated ability to frame an issue has been afforded to many publics – particularly due to the ability of these mediums to rapidly transmit and receive information. These affordances have the potential to be either beneficial or detrimental to a company when faced with a crisis. While an organization can benefit from strategic media relations and effective crisis communication, even the most established of firms can have their voice become convoluted or be reprimanded if communication is poorly executed.

This Masters Research Paper (MRP) will utilize the data breach experienced by Canadian online extramarital dating and social networking service Ashley Madison in 2015 as a case study to examine the extended impacts of managing organizational crises in an increasingly

interconnected and social media-driven context. Abutting the interconnected and social media-driven context lies a unique activism and morality incentive for the inception of the Ashley Madison data breach. Online hackers often target companies in the primary pursuit of intellectual property and thus, financial gain (Tuttle, 2015). Conversely, the Ashley Madison case embodies an uncommon pursuit: a socially and politically driven act based on the morality of a company's bottom line and security mishaps. The Ashley Madison hack has been dubbed as one of "the most attention-demanding example[s] of a trend in the expansion of what hackers recognize and target as valuable information" (Tuttle, 2015). This case study was chosen because Ashley Madison's controversial nature - for enabling extramarital affairs - offers an atypical framework for analyzing crisis management and recovery when it relates to online data breaches. The context by which Ashley Madison suffered from the crisis will be imperative to understand in uncovering whether or not effective crisis communication can come to the rescue - particularly when the existing public perception of a company is unapologetically negative.

This MRP, by drawing on Timothy Coombs' Situational Crisis Communication Theory (SCCT), will examine Ashley Madison's communication during the crisis – its successes and its failures – with an additional examination of the contentious perception held by the public towards the company prior to the crisis. Coombs' SCCT is particularly useful for such a study since it is an "evidence-based framework for understanding how to maximize the reputational protection afforded by post-crisis communication" (Coombs, 2007). This framework, in addition to Benoit's Image Repair Theory (1997), will guide the discussion about Ashley Madison's ability to build an effective response strategy and determine whether or not certain audiences or stakeholders might have enabled or disabled the company's ability to do so and recover.

1.1. Background of the Crisis

Ashley Madison is a company that since its inception was deemed by many to be controversial and immoral because of its facilitation of extramarital affairs. In 2015, Ashley Madison faced a targeted hack led by a social activist group called The Impact Team, who felt compelled to expunge the site from the internet since they regarded the site as immoral for not only facilitating illicit affairs, but also for having insecure and misleading content security measures. Specifically, The Impact Team claimed Ashley Madison's website to be "a scam with thousands of fake female profiles" (Adophia, 2015) to bolster their male users subscriptions into paid accounts. Additionally, The Impact Team sought to hack the company "in response to alleged lies [that Ashley Madison] told its customers about a service that allow[ed] members to completely erase their profile information for a \$19 fee (Krebs, 2015). According to The Impact Team, the "full delete" feature Ashley Madison advertised — which allowed for users to have their "site usage history and personally identifiable information from the site" removed — was a hoax (Krebs, 2015). Shortly after Ashley Madison refused to act on The Impact Team's threat to release user information (should the company fail to shut down operations), the hack took place, which led to the personal information of more than 37 million consumer profiles being released (Adophia, 2015). This release resulted in the credit card numbers, full/real names and addresses of Ashley Madison users worldwide being made accessible to the general public (Adophia, 2015). The direct impact that Ashley Madison's service and customers faced as a result of the hack embodied the term *hacktivism*, which refers to the "emergence of popular political action, of the self-activity of groups of people, in cyberspace" (Jordan & Taylor, 2004). More specifically, hacktivist groups are often motivated by a particular social or cultural phenomenon that they target online in hopes of their online efforts impacting the offline existence of the

phenomenon as well (Jordan & Taylor, 2004). The inception of hacktivism overlapped with the emergence of three divergent categories: “hacking, informational societies and modern social protest and resistance” (Jordan & Taylor). Hacktivism played a central role in Ashley Madison’s data breach, as “popular political action” was achieved through The Impact Team’s computer hacking (Jordan & Taylor, 2004). Additionally, the hack was particularly targeted by “the self-activity” of The Impact Team’s societal beliefs, insofar as the group sought to derail the company solely due to these beliefs, ultimately leading them to release the private consumer information.

The breadth of the data breach was immense and included substantial unintended externalities – not only did it lead to the release of the personal information of more than 37 million site users’, it also deeply affected the personal lives of many family members and colleagues who were not directly involved with the site. Over the course of user information being released, it was reported that “divorces, resignations, firings and suicides” (Syed & Cribb, 2018) were common throughout the series of events. While the magnitude of the data breach resulted in multiple negative outcomes, as previously mentioned, it is important to consider the controversial service offering Ashley Madison provided as central to the impetus of the data breach. Upon their initial launch in 2001, Ashley Madison faced negative public perceptions since “many of its users [were] married or in relationships, and unlikely to want their *cheating ways* publicly exposed” (Sorensen, 2015). This negative perception about the infidelity and “cheating ways” that Ashley Madison endorsed was often emphasized in media coverage during the crisis; for instance, *The LA Times* argued The Impact Team was “acting on moral grounds by exposing cheaters and hopeful cheaters” (2015) with their hack. In addition, Security News and Investigation publication, *Krebs on Security*, quoted The Impact Team speaking to their lack of

remorse and justification for the resulting hack. When speaking to the information released of Ashley Madison users, The Impact Team said “too bad for those men, they’re cheating dirtbags and deserve no such discretion,” and when addressing Ashley Madison, the hackers said:

“You promised secrecy but didn’t deliver. We’ve got the complete set of profiles in our DB dumps, and we’ll release them soon if Ashley Madison stays online. And with over 37 million members, mostly from the US and Canada, a significant percentage of the population is about to have a very bad day, including many rich and powerful people.” (Krebs, 2015).

These negative perceptions held about Ashley Madison coupled with the inception of the data breach ultimately compounded the crisis: how was this controversial company going to rebuild its public reputation in the face of such a communication calamity? Ashley Madison initially portrayed themselves as a “victim of cybercriminals” (Ward, 2015), however, it was not until The Impact Team further targeted them, exposing contentious emails from within the company (Ward, 2015) where the controversy peaked. These emails revealed former CEO Noel Biderman stating that Ashley Madison had hacked into another dating service in 2012 to gain competitor insight (Ward, 2015). Knowledge of this fraudulent behaviour was an additional factor in The Impact Team’s decision to expose Ashley Madison. Following the data breach and the widespread attention that the crisis received, there was a clear societal disruption created by the “sensitivity of the information exposed and its impact on affected individuals” (Office of the Privacy Commissioner of Canada, 2016), in addition to a lack of trust in the company.

Once the initial crisis event settled, the Office of the Australian Information Commissioner (OAIC) and the Office of the Privacy Commissioner of Canada (OPC) conducted a joint investigation into Ashley Madison’s privacy practices “at the time leading up to the data breach” (2016). The report ultimately revealed major oversight issues within Ashley Madison, including a lack of proper protocol for the safety and privacy of their users (2016). This

investigation was conducted in accordance with both Australia and Canada's Privacy and Information Protection acts and will be used as resources throughout this research to discuss the series of events in addition to key press releases and statements within the news media.

Literature Review

This literature review will discuss crisis communication theories that inform the research for this case study. However, a contextual framework will first be provided to introduce the terms 'crisis', crisis communication and crisis management as they relate to this case. Coombs' Situational Crisis Communication Theory (SCCT) will be the primary focus as it will guide the methodological framework used for qualitative analysis. Also, since SCCT is an evolution of Bernard Weiner's Attribution Theory, this too will be discussed. Finally, this literature review will discuss Benoit's Image Repair Theory since it will support the process of divulging Ashley Madison's ability to recover their reputation post initial crisis-event. The intention of leveraging both Coombs and Benoit's crisis communication theories is not to evaluate the strengths and weaknesses of each theory, but rather, leverage each theory for different aspects of the case.

2.1. Defining a "Crisis", Crisis Communication Theory & Crisis Management

To begin, it is important to first define the term 'crisis' and its specific relationship to crisis communication theory. However, a crisis can have different meanings depending on the context, thus making it difficult to assume one universally accepted definition in relation to crisis management for organizations (Carroll, 2009). In the journal *Defying a Reputational Crisis*, Carroll affirmed this contextual difficulty to be a result of competing perceptions held by the individual, group or organization at hand (2009). More specifically, these perceptual differences

in how one might understand a crisis can depend on certain political, technological and sociological contexts (Carroll, 2009). Similarly, Coombs' states that a crisis is "the perception of an unpredictable event that threatens important expectancies of stakeholders", which can not only severely hinder organizational performance, but also generate negative outcomes (Coombs, 2007). In addition, Smith and Elliot state a crisis is a "damaging event" or "series of events with emergent properties that [surpass] an organization's ability to cope with the task demands it generates" (2006). These authors also acknowledge crises to have "considerable implications for the organization and its stakeholders, in that damage can be financial, physical or reputational in scope" (2006). The financial, physical or reputational damage Smith and Elliot describe in relation to a crisis were confirmed results of the data breach crisis Ashley Madison faced. Not only were Ashley Madison's finances and reputation compromised by the hack, but more significantly, their most important stakeholders – namely its consumers – were compromised by having their private information made available to the public. While Smith and Elliot propose that a crisis can result in financial, physical or reputational damage, it is important to understand that regardless of the breadth in crisis – be it a 'minor localized disruption' or something denoting 'serious impact' – Coombs argues that there continues to be a "growing imperative for corporate social responsibility" (Coombs, 1999) in overall crisis management. Ashley Madison was often ridiculed for their lack of corporate social responsibility in that they had inappropriate security measures by not being prepared for a system hack such as this to occur. Moreover, the growing imperative for corporate social responsibility Coombs suggests in relation to crisis management is particularly applicable to Ashley Madison in that socially conscious activists — The Impact Team and those who accused Ashley Madison of immorality — were what initiated the crisis.

While a crisis is what “compels organizations to communicate with various audiences in order to limit the damages that may be caused” as a result, it is ultimately the quality of the communication during the crisis that is said to either “ameliorate or exacerbate the situation” at hand (Zaremba, 2015). As such, the implementation of crisis communication strategies involves the initial definition of the key stakeholders and audiences and then carefully communicating information to them through the most appropriate medium (Zaremba, 2015). Therefore, Crisis Communication Theory (CCT) is particularly motivated by analyzing the way an organization handles their image through both internal and external communication during a crisis and should be differentiated from the broader term Crisis Management (Johnson & Sellnow, 1995). Beyond the initial crisis communication, it is important to understand how rather than aligning public perception to a particular crisis response, crisis management operates at a higher level. Crisis management must employ a solution that “copes with the existing crisis”, while being mindful to avoid “similar crises in the future through ‘deliberative rhetoric’” (Johnson & Sellnow, 1995). Moreover, crisis management involves responding to feedback from audiences as well as evaluating the success of crisis communication efforts to determine effectiveness and then take efforts to plan for any further response required (Zaremba, 2015). Coombs argued that crisis management should be thought of as a process involving many parts including “preventative measures, crisis management plans, and post-crisis evaluations” (2012). To further establish a framework for crisis management, Coombs & Holladay developed a set of factors that embody its key constituents (2010). This framework took place through a three-staged approach — the pre-crisis stage, the crisis stage itself and the post-crisis stage (Coombs & Holladay, 2010) — and will be further discussed below.

Pre-crisis Stage

The pre-crisis is the first stage of crisis management when the organization must locate and reduce any potential risks to its operations; it is primarily concerned with not only being prepared, but also with taking every measure to prevent a crisis altogether (Coombs & Holladay, 2010). An additionally important term that lies at the core of crisis management prior to any crisis taking place is *signal detection* which if adopted and practiced properly, should “identify weak signals, [i.e.,] revealing that something is not as it should be” or “that something is developing in the wrong way” (Frandsen & Johansen, 2017). The previously mentioned Office of the Privacy Investigator’s report on Ashley Madison and their operations prior to the crisis will be leveraged to determine the company’s pre-crisis stage.

Crisis Event Stage

Coombs’ crisis event stage refers to when the “trigger event” occurs for the organization and it is divided into two parts: *crisis recognition* and *crisis containment* (2007). During the crisis event stage, Coombs suggests crisis managers must first understand the crisis as a “specific type” and then “use the crisis response strategies to establish a frame, or to reinforce an existing frame” (2007) based on the identified crisis. As soon as stakeholders begin to assess crisis responsibility, it is important to act quickly after determining what the crisis itself entails (Coombs, 2007). If organizations fail to insert themselves in the public domain in a timely manner through active response, they run the risk of reputational damage and the false spread of information, effectively devaluing any organizational communication to come. The crisis event stage will be intrinsic to understanding the Ashley Madison data breach and a pivotal point for analyzing their ability to set themselves up for image repair.

Post-crisis Stage

Coombs' post-crisis stage refers to the return of normal activities for an organization while still "providing follow-up information to stakeholders, cooperating with investigations, and learning from the crisis event" (Coombs, 2007). At this time, it is important for a company to resume normal operations, however, equally critical is the organization's continued effort in closely monitoring the situation (Coombs, 2007). More specifically, when an organization deems a crisis resolved, they must remain attentive to any ongoing and potentially upcoming threats similar in nature that would allow them to prepare for future, potentially negative, circumstances (Coombs, 2007). In addition, Coombs notes organizations must "update stakeholders on the business continuity efforts and deliver [on] all promised information" (2007) outlined during the crisis-event. At this point, an organization should keep three central tasks at the forefront to reinforce and or instill confidence: "dissect the crisis management effort, communicat[e] necessary changes to individuals, and provid[e] follow-up crisis messages as needed" (Coombs & Holladay, 2012) to assure audiences that the issue is still being actively attended to and considered for the future benefit of the company and its stakeholders. This stage is particularly interesting to consider in relation to the Ashley Madison data breach knowing the 'crisis event stage' peaked in 2015; by now in 2020, there is ample room for analysis of the post-crisis stage.

While the pre-crisis stage will be difficult to analyze, the crisis event and post crisis stages will be useful for analyzing the effectiveness of Ashley Madison's crisis communication efforts. However, given the social construction of the crisis, this research requires a contextual and evaluative approach to understand the company's specific crisis communication, making Coombs Situational Crisis Communication Theory (SCCT) an important guiding framework. As previously stated, SCCT provides "an evidence-based framework for understanding how to

maximize the reputational protection afforded by post-crisis communication” (Coombs 2007). In an effort to redefine the current landscape of academic research which, according to Coombs in 1999, lacked “proper knowledge and execution of crisis communication”, an applicable and empirical solution for this gap was developed through SCCT. SCCT’s empirical approach was compartmentalized through a system of three core elements in relation to the crisis itself, these include: 1) understanding the crisis situation and type, 2) acknowledging all potential crisis response strategies, and 3) strategically aligning a crisis response to the crisis situation at hand (Coombs, 2007). To advance the significance of SCCT in its initial development, Coombs highlighted Wartick’s (1992) notion that an organization’s reputation is the “aggregate evaluation stakeholders make about how well an organization is meeting stakeholder expectations based on its past behaviors” (Coombs, 2007). For Coombs, it is critical to first define the crisis situation, as it begs a strong understanding for the parameters, cause and evolution of the crisis from the outset, which can then better inform a crisis manager’s ability to leverage the most effective response strategy (Coombs, 2007). Having defined crisis communication, management and what a ‘crisis’ entails in relation, this literature review will continue the theoretical analysis of SCCT, by first divulging its roots in Attribution Theory.

2.2. SCCT and Attribution Theory

To develop an understanding of the roots of SCCT, it is important to consider how it is an evolution of *attribution theory*. More specifically, Coombs highlighted how attribution theory “provides the rationale for the relationship between many of the variables used” within SCCT (2007). Attribution theory argues that people have a natural tendency to assign responsibility for events - particularly negative in nature - that have taken place (Coombs & Holladay, 2010). SCCT builds upon this notion of assigned responsibility in that it seeks to predict the

“reputational threat presented by a crisis and prescribe crisis response strategies designed to protect reputational assets” accordingly (Coombs, 2007). This process helps direct the crisis manager to an understanding of how the “initial crisis responsibility” and assessment imparted on an organization is a direct result of stakeholder attribution (Coombs, 1999). When applying SCCT to crisis situations, Coombs emphasized that “the reputational threat to an organization increases as stakeholders’ attributions of crisis responsibility to the organization intensify” (1999). Attribution theory and thus SCCT, are particularly relevant to this literature review as Ashley Madison faced heightened public scrutiny for having a high crisis responsibility and, according to the Office of the Privacy Commissioner of Canada’s report (2016), for being legally responsible for the crisis. Building off of its initial roots in attribution theory, Coombs evolved SCCT by developing a core set of crisis types' to determine the level stakeholders use to attribute responsibility. These crisis types are grouped by three clusters: *the victim cluster*, *accidental cluster* and *the preventable cluster* (2007). First, the victim cluster is often caused by: natural disasters, rumours, workplace violence, or product tampering/malevolence (Coombs, 2007). In this category, not only the stakeholder(s), but the organization becomes a victim to the crisis. As a result, the organization faces a weaker crisis responsibility and a mild reputational threat associated to themselves (Coombs 2007). Similarly, organizational crises in the accidental cluster face minimal attribution of crisis responsibility; however, these types of crises typically include technical-error accidents, technical-product harm or challenges such as “stakeholders claiming an organization is operating in an inappropriate manner” (Coombs 2007). With the accident cluster, the crisis is considered an unintentional action by the organization. Conversely, the preventable cluster holds the greatest level of crisis responsibility in that the event is often considered purposeful or a result of a knowingly inappropriate action by the organization

(Coombs, 2007). Preventable (and sometimes considered ‘intentional’) crises are characterized by human-error accidents, human-error product harm, or organizational misdeed exhibiting either physical injuries, no injuries but deceit, or management misconduct (Coombs, 2007). According to Coombs, by identifying the crisis type, crisis managers can effectively anticipate and/or understand their level of crisis responsibility which will inform the response at the onset of the crisis (2007). Ashley Madison may not have identified themselves as solely responsible and accountable for the crisis, therefore, attribution theory as well as a more tactical application of crisis type and clusters will be important to determine effectiveness in their decision and approach to crisis communication.

2.3. Crisis and SCCT from a Stakeholder Perspective

Thinking beyond the crisis itself, it is important to consider how it operates bilaterally with perspectives and voices perpetuated by the general public and news media. This section of the literature review continues the discussion of a stakeholder’s perspective on a crisis through Coombs’ SCCT, as stakeholder perspectives and the news media are often the public framework for understanding current events and crises. Through the analysis of crisis communication literature, Holladay asserts the importance of an organization establishing ongoing and effective media relations so as to “positively influence press coverage and crisis framing” (2009). The ability to control and/or influence how a crisis is framed is highly valuable for any organization; it can directly influence stakeholder perceptions of the crisis and showcase how the organization is actively aware of and managing it (Holladay, 2009). While in some instances, the media may not be deemed a direct “stakeholder”, Koerber argues that when it comes to crisis management, the media should be considered a primary stakeholder “particularly due to their democratic role as watchdogs on government and business for citizens” (2017). Moreover, the growing

imperative for organizations to build a strong rapport with the media during a crisis comes at a time where news media have the ability to contextualize crises in certain ways which can lead to “blaming crisis events on specific individuals over other determinations” (Koerber, 2017). While the news media can contextualize and frame a crisis, it is important to note that it is not only the news media that have the capability to generate a mass public opinion. With the current mediated landscape today coming with “myriad accessible communication channels at [our] disposal”, Koerber argued that stakeholders during a crisis are even more influential compared to the landscape a decade ago (2017). This new-found ability of stakeholders to influence opinion is certainly important to consider when discussing SCCT theory, as subjective stakeholder opinions (like that of The Impact Team’s) can become active contributors to the ‘making’ of a crisis. It will be important to consider the level of communication The Impact Team had with the news media versus Ashley Madison when determining the role of the stakeholder in framing a crisis.

Based on the theories provided thus far, the implementation of a sound crisis communication and response strategy is an integral component to crisis communication and management. While it is clear effective media relations might help limit negative media coverage for an organization, certain news frames may still persist and undermine an organization’s crisis communication efforts. When understanding crisis communication and Ashley Madison’s crisis, certain news frames/perspectives can highlight how information might become presented through specific agendas to the public. However, an organization can also actively monitor developing narratives in order to inform and guide their communication strategies throughout the duration of a crisis. Given Ashley Madison’s public perception was seen as controversial by many from the outset, it is important to consider how certain platforms and news media

discussed the series of events taking place and whether or not certain frames or subjectivities were intertwined when analyzing the overall effectiveness of their response.

2.4. Crisis Response: SCCT and Image Repair Theory

Having discussed SCCT and attribution theory as well as how crises might be framed by different stakeholders, the following portion of this literature review will focus on theory-based communication tactics and strategies in response to crisis situations. Specifically, it will compare Benoit and Coombs' crisis response strategies as well as their ability to affect public perception.

When discussing different communication approaches during a crisis, Benoit emphasized the importance of delivering a consistent message that offers compelling support and if/when a wrongful act is committed, issuing a prompt apology and corrective action where necessary (1995). In a qualitative case study with image repair strategies tested and applied, Benoit revealed many communication errors when a large national auto-repair chain, Sears, sought to manage charges of consumer fraud. Findings by Benoit revealed an “unfavourable evaluation” of Sears' crisis communication discourse due to their inconsistent, contradictory statements: first, Sears attacked their accuser, effectively denying any wrongdoing, then later dropped the attacks and admitted that corrective action would be made (1995). By not maintaining consistency in communication and response strategies, the overall response from the organization was not only rendered discreditable, but it invited immense suspicion from stakeholders (1995).

In its initial development, Benoit (1997) coined what is now Image Repair Theory (IRT) as Image Restoration Theory. The switch from *restoration* to *repair* came as a result of Benoit thinking the previous title might “inadvertently imply that one can or should expect to be able to *completely* restore an image” by using the intended strategies, effectively “[obliterating] any stigma in the image” (Benoit, 2015). Benoit's distinction with “repair” assumes any effort to

fully “repair” an image can still take place, however it does not necessarily imply that a “complete restoration is always possible, or [perhaps] even the only desirable outcome” (Benoit, 2015). Given image repair discourse is a “form of communication” in itself, Benoit posited the importance in understanding the *nature* of communicating first, before understanding how to create image repair (2014). The nature of persuasion is an additional, yet equally important, component to Benoit’s IRT: it emphasizes how an organization can persuade an audience and reshape their perception. Benoit’s notion of a “persuasive attack” is particularly relevant to the Ashley Madison crisis as it is viewed as a message “that attempt[s] to create unfavourable attitudes about a target (person or organization)” (2015). As such, persuasive attacks can prompt the need for image repair and are acts of “subversion, or messages intended to damage an image” (2015). Specifically, The Impact Team and their attempt to strengthen the belief of Ashley Madison and the unfavorable value of infidelity exemplifies a “persuasive attack” in action.

To continue the discussion of Benoit’s image repair strategies during a crisis, below are the five core categories for response which have been widely accepted for their sound execution of a crisis communication strategy, three of which include more specific, tactical approaches. For the purpose of application and additional understanding, these strategies and corresponding tactics have been illustrated using a potential, albeit made-up response, by Ashley Madison.

Table 1. Benoit’s Typology of Image Repair Strategies

Broad Strategy	Tactic	Examples: Leveraging Ashley Madison Data Breach
Denial	<i>Simple Denial</i>	The threats of a hack into the Ashley Madison database are unfounded. Our systems are secure and no user information will be compromised.
	<i>Shift Blame</i>	The illegal hacker must be held responsible for this act of extortion, not our company.
Evasion of Responsibility	<i>Provocation</i>	We only created fake female profiles on our dating site to make men feel more comfortable with their infidelity experience. There was a lull in female subscriptions so we didn’t want to lose our valued, male members.
	<i>Defeasibility</i>	We had no control over the hack into our system as no Government regulations were in place to prevent the illegal hackers from infiltrating our site.
	<i>Accident</i>	We truly believed our systems were completely secure and would never have wished for our customers to become exposed.

	<i>Good Intentions</i>	We didn't deactivate our customers' user accounts to safeguard their information once we received the initial threat from the Impact Team because we intended to correct the issue before it escalated.
Reduce Offensiveness	<i>Bolstering</i>	We have always put customer satisfaction at the forefront. We know this is true because of the magnitude of loyal members we have and continue to support in their everyday romantic lives.
	<i>Minimization</i>	In today's current climate, many businesses are facing illegal hacks into their systems everyday just like us.
	<i>Differentiation</i>	We only created fake female accounts for a short period of time, and had full intention of removing them once our female numbers went back up.
	<i>Transcendence</i>	The hackers threat to expose our user information if we do not shut down as a company was not a possibility. We value our customers too much to get rid of the service we provide them. Instead, we have employed top-notch security to ensure no hack occurs.
	<i>Attacking one's accuser</i>	The threat from The Impact Team is not real - we will not let internet trolls affect people's perception of Ashley Madison as a secure company.
	<i>Compensation</i>	For those whose personal lives have been affected by the release of private information, we will be offering \$3,000 to recompense for any harm caused.
Corrective Action	No specific tactic	We regret the release of our users information and promise to repair all damage caused by the data breach. Our website has since shut down and will only turn back on once we've ensured it is safe and our affected users have been properly compensated. For the time being, we have developed a public microsite that provides extensive, on-going information about our current undertakings to remedy the situation.
Mortification	No specific tactic	We deeply apologize for any and all inconvenience caused by the data breach and understand that it is Ashley Madison's responsibility and promise to its users to ensure a secure platform.

*Repair strategies from Benoit, W. *Accounts, Excuses, and Apologies: Image Repair Theory and Research*. 2014.

State University of New York Press.

Together, Benoit's five image repair strategies offer a framework for certain types of discourse that can guide and inform persuasive messaging during a crisis. Benoit explained that these image repair strategies work most effectively when "viewing the image repair event in terms of the elements of attacks" i.e., beliefs/blame and offensiveness/values" (2014). As such, the communicator must understand the current stakeholder audience prior to an image repair strategy being employed (Benoit, 2014). Aside from *corrective action* and *mortification*, Benoit's strategies work to reduce 'perceived responsibility' of an organization in relation to the crisis and thus "mitigate the damage to reputation" (2014). Through IRT, Benoit's strategies are uniquely distinguishable through their direct pursuit of "persuasion" in that their approach to crisis response attempts to "alter or create new beliefs within an audience" (2014). When discussing IRT strategies in comparison to Coombs' SCCT strategies, Benoit identified one key reservation against SCCT in that it "assumes the crisis type can be determined a priori" (2014).

While reinforcing the belief that a crisis type might be easily applied in some instances, Benoit argued that a perception of reality is ultimately socially constructed through messages, reinforcing his emphasis on *persuasion* for IRT. To effectively understand and compare Benoit's IRT with Coombs' SCCT strategies, provided below are Coombs' core response strategies with a sample application to Ashley Madison, as conducted with Benoit's strategies.

Table 2. Coombs' SCCT Crisis Response Strategies by Response Option

Response Option	Tactic	Examples: Leveraging Ashley Madison Data Breach
Deny	<i>Attack the accuser</i>	Ashley Madison released a public statement confronting the alleged hackers into its system, highlighting how it is an illegal act and they must not move forward.
	<i>Denial</i>	The threats to Ashley Madison's system are unfounded, no hack of the system will actually take place.
	<i>Scapegoat</i>	Any hack into our secure system would be a violation of the law. Our security measures are properly implemented to protect our customers and a violation of that would be criminal.
Diminish	<i>Excuse</i>	Despite all security measures, Ashley Madison has unfortunately had no control over the hack taking place. It is a true cyber-crime.
	<i>Justification</i>	Companies all across Canada are unfortunately facing the same problem of cyber-criminals and potential hacks into their systems.
Deal	<i>Ingratiation</i>	We have always put customer satisfaction at the forefront. We know this is true because of the magnitude of loyal members we have and continue to support in their everyday romantic lives.
	<i>Apology</i>	We deeply apologize for any and all inconvenience caused by the data breach and understand that it is Ashley Madison's responsibility and promise to its users to ensure a secure platform.
	<i>Concern</i>	Our customers are our biggest priority - as such, Ashley Madison's website has been shut down and will only turn back on once we've ensured it is safe and our affected users have been properly compensated. For the time being, we have developed a public microsite that provides extensive, on-going information about our current undertakings to remedy the situation.
	<i>Compensation</i>	For those whose personal lives have been affected by the release of private information, we will be offering \$3,000 to recompense for any harm caused.
	<i>Regret</i>	We deeply apologize for any and all inconvenience caused by the data breach and understand that it is Ashley Madison's responsibility and promise to its users to ensure a secure platform. We are doing everything in our power to repay our customers and ensure they are properly compensated for this tragic event.

*Response strategies retrieved from Coombs, T. *The Protective Powers of Crisis Response Strategies: Managing Reputational Assets During a Crisis*. 2006. *Journal of Promotion Management*.

As displayed in the above chart, Coombs' three crisis response 'options' deny, diminish and deal were sub-categorized by ten tactical approaches (2006). According to Coombs, the decision and consequent action of deploying a certain strategy must only occur if a proper understanding of the level of crisis responsibility and crisis type has taken place (2012). Similar to IRT, SCCT uses communication to defend reputation and much like IRT, is crafted to

“understand the communication options available for those, whether organizations or individuals, who face threats to their reputation” (Benoit, 2014). Perhaps most significantly, Coombs highlighted how IRT’s recommendations of emphasizing the apology and accepting responsibility for the crisis were what informed SCCT the most (Coombs & Holladay, 2010). However, it is important to revisit Coombs’ more contextual analysis which includes: understanding what potential intensifying factors for the crisis exist -- i.e., the organization's crisis history and/or its prior reputation (Coombs & Holladay, 2010). This is an important step that Coombs integrates as it might change stakeholders’ attribution of crisis responsibility. From here, a communicator can then pursue a crisis response.

Benoit’s IRT strategies in some ways parallel Coombs’ SCCT strategies, however, their foundational applications ultimately differ in their roots – *persuasion* vs. *situation*. The research for this paper will primarily apply Coombs SCCT to look at the crisis situation that engulfed Ashley Madison. However, Benoit’s argument that a crisis response according to SCCT must primarily be informed by the crisis situation and type fails to holistically consider the audience’s beliefs and values as well as the fact that “different people in the audience can have different sets of beliefs and values” (2014) will also be considered.

Research Questions

1. How can Ashley Madison’s crisis management during the ‘crisis event stage’ be interpreted using Coombs’ SCCT framework? According to SCCT, was Ashley Madison’s crisis response strategy effective?
2. To what extent might Benoit’s notion of ‘perceived offensiveness’ and ‘multiple audiences’ have enabled or disabled Ashley Madison’s crisis response?

Method of Analysis

Through an interpretative, constructionist approach, this research paper will critically analyze the Ashley Madison data breach through a single qualitative case study. Scheurman and Evans (2018) explain that examining phenomena using a constructivist lens is to examine phenomena as:

Not simply something immutably out there in the world but rather, [a]s constructed inter-subjectively in a manner that reflects (a) our own personal needs and habits, (b) the established norms and presuppositions of the culture in which we must live, and (c) the constraints imposed by the established society of which the culture is an expression. (2018)

While the Ashley Madison case exemplified how imperative preemptive crisis management is for a company whose consumers expect their private information to be upheld, this research will consider the notion of constructivism in that the views held about Ashley Madison prior to the crisis were socially constructed. Moreover, it is important to consider that viewpoints about Ashley Madison as a company may have evolved and/or shifted as a result of press releases, competing news sources and blogs discussing the crisis throughout its duration. Additionally, it is important to note that the Ashley Madison data breach received international, widespread attention, which resulted in a large amount of online news and other media that could not have been analyzed within the scope of this MRP. As such, this research will not seek to determine which perspective is necessarily correct but instead, leverage Coombs SCCT and Benoit's IRT to determine the effectiveness of Ashley Madison's direct communication with audiences.

Prior to executing the data collection, the timeframe between each piece was noted as an additional point of analysis in comparison to the continuation of events noted through news articles. Therefore, the textual analysis will follow a chronological path – first by collecting the

initial press release provided by the company and then other communication material that followed. In order to employ a qualitative, discourse analysis of Coombs' SCCT strategies in conjunction to Benoit's notion of 'perceived offensiveness' and 'multiple audiences', the below data/content (Table 3) will be analyzed.

Table 3. Content for Data Collection and Analysis

1.	Ashley Madison's initial press release.
2.	Select statements in mainstream media articles discussing the event in the following month with quoted communications from Ashley Madison and The Impact Team.
3.	Statements from Ashley Madison found in news articles a month after the crisis event, noting briefly Ashley Madison's CEO departing.
4.	A press release from one year after the crisis event.

This research will examine the sources indicated above through textual analysis and coding according to Coombs crisis response strategies to address research question one. Further, this data collection will be guided by Coombs' three-stage approach to crisis management to understand how the crisis situation was handled. As previously stated, the joint investigation made by the Office of the Australian Information Commissioner (OAIC) and the Office of the Privacy Commissioner of Canada (2016) will also be utilized as a key source for understanding events with additional news articles including quoted statements from Ashley Madison and The Impact Team for this research.

In order to address research question two, it will be essential to critique news releases and/or statements made by Ashley Madison to determine whether or not they addressed different audiences appropriately and whether or not they align with Benoit's IRT strategies of persuasion and argument for 'multiple audiences'. Given the end result of Ashley Madison having faced a

lawsuit for internal misconduct and improper security measures (Office of the Privacy Commissioner of Canada, 2016), it will be important to analyze how Ashley Madison discussed their misconduct and security measures to determine if truth and transparency were central to their narrative.

To structure the qualitative analysis and findings for this case study, Coombs' empirically tested method of SCCT will be utilized as the primary framework to determine the crisis situation, crisis response strategies and an appropriate system for matching the crisis situation to crisis response strategies (Coombs, 2006). By leveraging these three steps, research question #1 will be addressed by interpreting Ashley Madison's crisis management during the 'crisis event stage' and whether or not their response strategy was effective. To address research question #2, an application of Benoit's IRT strategies of persuasion will be evaluated, and depending on whether or not Ashley Madison's communication addressed 'multiple audiences' or the notion of 'perceived offensiveness', a continued analysis for the effectiveness of their crisis response will be reached.

Overall, the series of events and corresponding responses by Ashley Madison will be structured through Coombs' integrative three-staged approach to crisis management:

1. **The Pre-Crisis Stage:** Signal Detection, Prevention, and Preparation;
 2. **The Crisis Stage:** Recognition, Containment, and Restitution; and
 3. **The Post-Crisis Stage:** Evaluation, Institutional Memory, and Post-Crisis Actions
- (Coombs, 1999).

Qualitative Analysis and Findings

5.1. Pre-Crisis Stage

While the focus of this MRP's findings remain on the crisis event stage, a brief analysis will identify key findings from the pre-crisis stage to determine Ashley Madison's level of preparedness. To begin, the pre-crisis stage must include analysis of the organization's success in properly preparing for a crisis. The first tactic within the pre-crisis stage being 'signal detection' — which includes the identification of 'weak signals' for anything seemingly not as it should be, or developing in the wrong way (Frandsen & Johansen, 2017) — was not an intrinsic component within Ashley Madison's operations ahead of the data breach. This was largely due to the abrupt nature of the system hack, followed by continued threats from The Impact Team to release their proprietary consumer information. The report on the case from the Office of the Australian Information Commissioner (OAIC) and the Office of the Privacy Commissioner of Canada (OPC) confirmed the sudden and unanticipated nature of this event on July 25, 2015 stating that:

The Impact Team threatened to expose the personal information of Ashley Madison users unless Ashley Madison shut down [their website]. Ashley Madison did not agree to this demand. (2016)

On the day Ashley Madison's employees were informed of the hack, they were greeted upon logging into their computers by a "ransom message" noted to be accompanied by "the AC/DC song, Thunderstruck" (Lord, 2017) from The Impact Team. Ashley Madison was blindsided by The Impact Team's sudden threat and infiltration into their system however, it would be inaccurate to conclude that the company did *not* consider the possibility of a data breach prior to its occurrence and that they lacked Coombs' component of 'signal detection' within the Pre-Crisis stage. However, findings from the OPC report regarding Ashley Madison's security

safeguards uncovered that despite Ashley Madison's "a range of security safeguards to protect the personal information it held," their underlying security framework lacked the following key elements:

- a. Available and properly "documented information security policies or practices";
- b. "An explicit risk management process", which included "periodic and proactive assessments of privacy threats, and evaluations of security practices to ensure Ashley Madison's security arrangements were "fit for purpose"; and lastly,
- c. Adequate security and privacy training to "ensure all staff were aware of, and [able to] properly carry out their privacy and security obligations appropriate to their role and the nature of Ashley Madison's business" (OAIC, OPC, 2016).

This indicates that not only did Ashley Madison fail to implement the correct preventative and crisis preparation measures - especially considering "the sensitivity of the personal information under PIPEDA" - they also failed to take "reasonable steps in the [given] circumstances to protect the personal information [they] held" under the privacy acts (2016). It can therefore be concluded that Coombs 'prevention and preparation' guidelines within the pre-crisis stage were not at the forefront of Ashley Madison's crisis communication strategy.

5.2 The Crisis Stage

The key findings provided through the analysis of the crisis event stage will be compartmentalized through Coombs' three micro-stages of the crisis event: Recognition, Containment, and Restitution (2007).

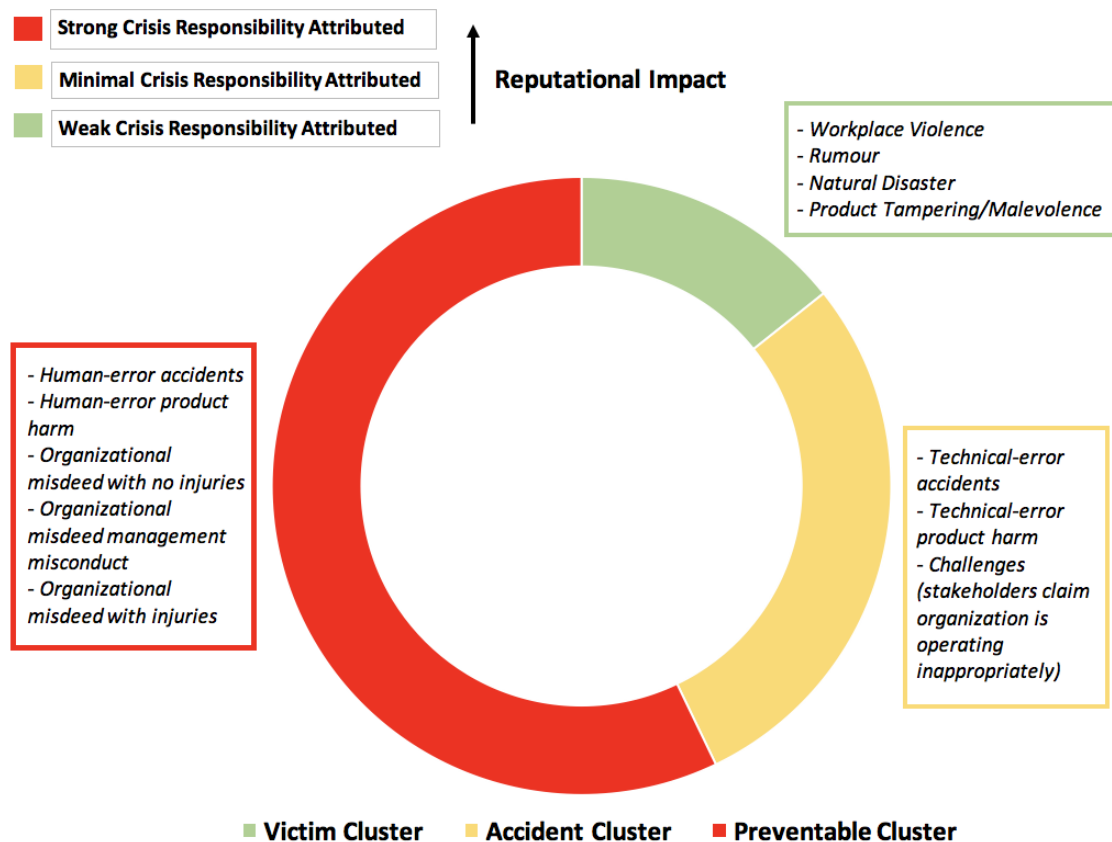
1. Recognition

As mentioned in the literature review, SCCT posits that recognition of the *type* of organizational crisis and situation must be the focus for any company when first faced with a crisis prior to releasing any communications to the public. By first determining the type of crisis

at the outset, organizations are able to understand their “foreseeable rank of crisis responsibility” and consequently, the level of responsibility a stakeholder might attribute against them (Coombs, 2007). Once the type of crisis and situation has been properly identified, an optimal response can be developed and disseminated. To recognize Ashley Madison’s crisis type, Coombs’ three core ‘crisis clusters’ will be defined and applied below.

The below chart showcases the three overarching crisis clusters: 1) victim, 2) accident and 3) preventable/intentional. The legend at the top left showcases the level of crisis responsibility attributed to each cluster — red being the greatest, green being the lowest — and thus, the level of reputational threat the organization will likely face. Included within the coloured boxes in the chart’s parameter are specific crisis types that embody each cluster.

Table 4. SCCT Crisis Types by Crisis Clusters



**Note.* Information used to create the above display chart retrieved from “Protecting Organization Reputations During a Crisis: The Development and Application of Situational Crisis Communication Theory.” by W. T. Coombs, 2007, Corporate Reputation Review, 10(3).

The foundation in which crises are classified will provide the basis for analyzing the crisis-event stage of this case study. When determining the optimal response strategy for an organization in crisis, SCCT asserts that crisis managers must select their strategy based on the specific framing that the crisis has been situated within, which can be determined using table 4 above (Coombs, 2007). Upon initial impression, the Ashley Madison crisis appeared to possibly embody two separate clusters: the victim cluster and the preventable cluster. However, further analysis concluded this crisis to be emblematic of the preventable cluster. The findings which lead to this conclusion are provided below.

a) The Victim Cluster

The Ashley Madison data breach was considered to fall within the victim cluster, particularly as the cluster is defined by an “external agent [causing] damage to an organization” and includes “product tampering” (Table 4). Due to the crisis arising as a result of an external agent (The Impact Team), damaging Ashley Madison by tampering with their product/service offering, this assumption was made. Furthermore, in a news report released one month after Ashley Madison became informed of The Impact Team’s threat, it was stated that under Canadian law, The Impact Team could face criminal charges such as:

- **Theft:** due to the “proprietary interest in the data”
- **Mischief to property:** due to the “obstruct[ion], interrupt[ion], or interfere[nce] with the lawful use, enjoyment or operation of property”
- **Mischief in relation to computer data & Extortion:** Due to The Impact Team threatening Ashley Madison to take down its website/service permanently or their private customer records/profiles would be released

- **Criminal harassment:** “Depending on the way in which it’s been leaked or published”; and lastly,
- **Intimidation.** (Schwartz, 2015).

While the above charges could be construed to imply that Ashley Madison was a *victim* to the theft, extortion and harassment brought on by the breach, the article also noted that for the police to identify and arrest The Impact Team, they would have to undertake a “long and complex investigation,” prior to formally laying charges (Schwartz, 2015). These potential indictments and charges identified under Canadian Law might support Ashley Madison’s victim approach/response however, the avoidable damage Ashley Madison faced by “the external agent” (The Impact Team) remains. In addition, despite Ashley Madison and its users’ security and privacy being compromised, the OPC/OAIC report noted that a security compromise of this nature does not necessarily “point to a contravention of PIPEDA or the Australian Privacy Act” (2016). While the hack and consequent damage might have made Ashley Madison the initial ‘victim’, previous findings stated in the pre-crisis stage regarding Ashley Madison’s lack of crisis preparedness and security framework render this assumption falsifiable. In addition, concluding Ashley Madison as a sole ‘victim’ to the hack would fail to address the underlying issues intrinsic to the company’s operating software and security measures.

b) The Preventable Cluster

Results from the OAIC and the OPC report proved Ashley Madison’s fundamental issue to be their lack of adequate safeguards “to protect the personal information of [their] users” (2016). The report further highlighted the ‘preventable’ nature of the crisis when stating:

It is not sufficient for an organization such as Ashley Madison, or any organization that holds large amounts of personal information of a sensitive nature, to address information security without an adequate and coherent governance framework. (OAIC, OPC, 2016)

The crisis ultimately falls under Coombs' 'preventable cluster' as Ashley Madison "knowingly [took] inappropriate actions" to prevent the breach and had their internal procedures consist of "human error [which] could have been avoided" (Table 4) (Coombs, 2007). While Ashley Madison initially became a victim to hacking and threats, the company failed to recognize the potential for a data breach of this magnitude, and in doing so, failed to implement proper crisis, risk communication tactics, or cautionary blockades within their software. These failed efforts ultimately rendered their crisis as one that could have been prevented from the outset.

2. Containment

With part one (recognition) of the three stages within the crisis event analyzed, the level by which Ashley Madison sought to communicate how and what they were doing to address and remedy the crisis through containment will now be discussed.

When evaluating how to contain a crisis, Coombs highlighted the importance of an organization's initial response, in that it must be quick, accurate, confident and demonstrate how the organization's "not only in charge, but capable of handling [it]" (2007). Given this key tenet of containment and thus organizational recovery, it is important to note Ashley Madison's response to the data breach was not made public until July 20, 2015, five days after the notice of a potential hack into their system. While Ashley Madison's initial response lacked Coombs' prefatory suggestion of immediacy, a detailed analysis of the company's ability to contain the crisis based on their first public response/press release will be conducted. In addition to discussing Ashley Madison's ability to provide an accurate and accountable statement to guide stakeholder understanding of crisis management, Coombs' (2007) "three types of instructing information" that stakeholders are required to know will first be applied. Ashley Madison's initial public-facing communication after the crisis-event took place on July 20, 2015, and is

provided below for reference.

Table 5. Ashley Madison’s Initial Press Release

Statement From Avid Life Media Inc.

NEWS PROVIDED BY
Avid Life Media, Inc. →
Jul 20, 2015, 02:17 ET

SHARE THIS ARTICLE



TORONTO, July 20, 2015 /PRNewswire/ -- We were recently made aware of an attempt by an unauthorized party to gain access to our systems. We immediately launched a thorough investigation utilizing leading forensics experts and other security professionals to determine the origin, nature, and scope of this incident.

We apologize for this unprovoked and criminal intrusion into our customers' information. The current business world has proven to be one in which no company's online assets are safe from cyber-vandalism, with Avid Life Media being only the latest among many companies to have been attacked, despite investing in the latest privacy and security technologies.

We have always had the confidentiality of our customers' information foremost in our minds, and have had stringent security measures in place, including working with leading IT vendors from around the world. As other companies have experienced, these security measures have unfortunately not prevented this attack to our system.

At this time, we have been able to secure our sites, and close the unauthorized access points. We are working with law enforcement agencies, which are investigating this criminal act. Any and all parties responsible for this act of cyber-terrorism will be held responsible.

Avid Life Media has the utmost confidence in its business, and with the support of leading experts in IT security, including Joel Eriksson, CTO, Cycura, we will continue to be a leader in the services we provide. "I have worked with leading companies around the world to secure their businesses. I have no doubt, based on the work I and my company are doing, Avid Life Media will continue to be a strong, secure business," Eriksson said.

SOURCE Avid Life Media, Inc.

To begin, the above press release provided a limited account of the “instructive information” that Coombs deems imperative to properly handle crisis communication. Ashley Madison provided minimal information relating to the ‘crisis basics’ that a company must communicate to its audience during a crisis. While the second and third ‘instructing pieces of information’ were provided (protection and correction), their inclusion was insufficient and brief. These three conclusions are detailed below.

1. **Crisis Basics.** Ashley Madison's explanation of events during the initial crisis to the public was woefully vague. The company's initial press release noted that the organization was "recently made aware of an attempt by an unauthorized party to gain access to [their] systems", but they did not provide additional insight or specific information about the hack to the public or their customers.
2. **Protection.** In their initial press release, Ashley Madison did not articulate any direct concern for the protection of their users from further harm/exposure. Instead, the company stated how at that point, they were able to "secure [their] sites, and close the unauthorized access points" (Avid Life Media, 2015). In addition, the response continued to state how moving forward, "they were working with law enforcement agencies" in order to investigate the "criminal act" (Avid Life Media, 2015). Rather than articulating the human desire to protect their customers at a time of great uncertainty, Ashley Madison stated that "the current business world has proven to be one in which no company's online assets are safe from cyber-vandalism" (2015). In doing so, Ashley Madison alluded to a strategy that *minimized their blame* in the crisis event, instead of taking the opportunity to meaningfully address the steps they could have taken to ensure the protection of their consumers personal information.
3. **Correction.** Ashley Madison did state what they were doing to correct and prevent a repeat of a crisis in that they were "immediately launch[ing] a thorough investigation utilizing leading forensics experts and other security professionals to determine the origin, nature, and scope of this incident" (Avid Life Media, 2015). However, the events following the press release rendered this statement falsifiable. No more than two days after the first press release, The Impact Team revealed "the names and

information of two Ashley Madison users — a man from Brockton, MA and a man from Ontario, Canada — in the first data leak to come from the hack” (Digital Guardian, 2015). Two days after ensuring that they had secured their system and launched forensic and security professionals to determine the cause of the incident, their access points were confirmed to still be vulnerable, contrary to their initial statement.

Initial Crisis Response Strategies

To further analyze the initial press release and ‘Crisis Event Stage’, Coombs’ crisis response strategies have been textually applied to Ashley Madison’s initial press release. The following strategies for the analysis were considered: 1) Express Concern for Victims, 2) Attack the Accuser, 3) Denial, 4) Scapegoat, 5) Excuse, 6) Justification, 7) Compensation, 8) Apology, 9) Regret, and 10) Ingratiation and 11) Victimage (Coombs, 2007). The initial press release most prominently applied to 5 out of the 11 crisis response strategies, which are analyzed below.

- **‘Scapegoat’ and ‘Victimage’ Response Strategies** – Ashley Madison demonstrated both the ‘scapegoat’ and ‘victimage’ response tactics in their initial press release by immediately criminalizing The Impact Team, effectively deeming the hackers as the perpetrator. Ashley Madison exemplified this strategy by forcefully labelling the hack “criminal” in nature; for instance, Ashley Madison stated they were “working with law enforcement agencies, to investigate the *criminal act*”, ensuring “those responsible for the act of “*cyber-terrorism*” would be held responsible” (2015). This response strategy effectively shifted ethical responsibility onto The Impact Team, who according to Ashley Madison, were guilty of serious misconduct, in comparison to Ashley Madison’s self-assessment as a victim.

- **‘Excuse’ and ‘Justification’ Response Strategy** – Ashley Madison adhered to the ‘excuse’ and ‘justification’ response strategy as they “minimized organizational responsibility by denying any intent to cause harm” and by alluding to their inability to “control the events that triggered the crisis” (Coombs, 2007). In addition, these strategies were exemplified when the company stated that: “the current business world has proven to be one in which no company's online assets are safe from cyber-vandalism, with [Ashley Madison] being only the latest among many companies to have been attacked, despite investing in the latest privacy and security technologies” (2015). This statement ultimately minimizes the company’s attribution of responsibility for the crisis as Ashley Madison emphasized how, despite their best efforts and use of the latest security technology, there was nothing they could have done to prevent it. The press release continued to “minimize organizational responsibility” by “denying intent to do harm” when stating how despite always having placed the confidentiality of their customers' information at the forefront, “as other companies have experienced”, their security measures “unfortunately could not have prevented the attack” into their system (Ashley Madison, 2015). By leveraging and communicating the fact that other companies often experience unforeseeable data breaches as well, this response can be viewed as both an excuse to minimize their perceived responsibility over the situation but also a justification of its occurrence to their stakeholders. Moreover, Ashley Madison further utilized the justification tactic when highlighting their long-term dedication to ensuring leading IT vendors were on-board prior to the hack. This statement reinforced to the reader their ‘dedication’ to security, and sought to lessen the chance of public assumption that they did not do enough to protect their software.

- **Ingratiation** – Ashley Madison utilized the ingratiation response strategy when stating that they always had “the confidentiality of [their] customers’ information foremost in [their] minds, and had stringent security measures in place, including working with leading IT vendors from around the world” (2015). Similar to the justification strategy, this statement highlighted the criminal and unpreventable nature of this hack, noting Ashley Madison’s past “good works of the organization” (according to Coombs’ ingratiation strategy) for always having had leading IT vendors operating for them across the globe.

Most notably, the crisis communication strategies not included in the analysis above were compensation, regret and apology. Specifically, Ashley Madison communicated no effort to offer compensation of any form to the affected individuals from the breach, and thus, did not adhere to the “compensation response strategy”. In addition, the “regret response strategy” was not exercised, with Ashley Madison making no effort to express remorse, nor communicating that they “[felt] bad about the crisis” (Coombs, 2007). Lastly, the “apology response strategy” was considered for this analysis as Ashley Madison did briefly state: “we apologize for this unprovoked and criminal intrusion into our customers’ information” (2015). However, the apology ultimately failed to adhere to Coombs’ definition of what the ‘apology strategy’ indicates whereby an organization must take “*full* responsibility for the crisis and/or ask[s] for forgiveness from their consumers” (2007). Ashley Madison’s apology was limited in multiple ways: it insinuated that the breach was brought upon as an ‘intrusion’ by criminals, and that it was out of their control, therefore not qualifying for the organization’s responsibility and accountability.

3. Restitution

The next component in Coombs SCCT, following crisis containment, is the restitution phase. This part of the analysis will discuss additional Ashley Madison communication pieces in the events and news articles following their initial crisis response as previously discussed.

‘Victimage’ Response Strategy, ‘Attack the Accuser’ Strategy

Following Ashley Madison’s initial press release, it was reported that on August 18, 2015, the company’s “entire customer database was indeed put online, including the details of approximately 36 million Ashley Madison user accounts” (Lamont, 2016). However, throughout the “beginning weeks of the crisis”, Ashley Madison allegedly “stopped responding in any sort of adequate way to calls and emails from its terrified customers” and instead provided limited, unrelated and short press releases (Lamont, 2016). The aforementioned statements provided by *The Guardian* regarding Ashley Madison’s public facing communications activity exemplify Coombs’ ‘victimage’ response strategy in that the company both directly and indirectly reminded the public that they were not assuming responsibility for the crisis - ultimately perpetuating the narrative from their initial press release. Moreover, in a report from the CBC on August 19, 2015 following additional released data which “appeared to be the credit card numbers and other sensitive information of Ashley Madison's customers online”, the company was quoted to have again labelled this release of data "an act of criminality" (Adophia, 2015). The news article quoted the following statement from Ashley Madison:

It is an illegal action against the individual members of AshleyMadison.com, as well as any freethinking people who choose to engage in fully lawful online activities. The criminal, or criminals, involved in this act have appointed themselves as the moral judge, juror, and executioner, seeing fit to impose a personal notion of virtue on all of society. (Adophia, 2015)

In this statement, Ashley Madison reminded the reader how those who hacked their system should face severe consequences for their corrupt personal ideology, and how their act impacted members who were engaging in “fully lawful online activities” (Adophia, 2015). The news article continued to quote Ashley Madison saying they would “not sit idly by and allow [those] thieves (The Impact Team) to force their personal ideology on citizens around the world” (Adophia, 2015). Coombs discussed the ‘victimage’ response strategy to be a tactic that “reinforce[s] the belief that an organization deserves sympathy” (2007). This tactic was utilized by Ashley Madison as they sought to reinforce the narrative of how they were targeted by thieves with a subjective personal interest, of which their innocent consumers had to suffer from.

‘Scapegoat’ Response Strategy

Three days after the release of the aforementioned statement, CEO Noel Biderman resigned with Ashley Madison releasing a brief statement to announce his departure. At this point in time, the company noted no further “instructive information” regarding the crisis. Instead, they merely acknowledged that their “existing senior management team [would] take the helm for now”, and reiterating how they were “still working with law enforcement to track down the hackers who posted data from internal company documents and 36 million user accounts online on Aug. 18” (Garcia, 2015). This statement expressed no sense of apology, concern or guilt towards their customers. In addition, *The Globe and Mail* reported a few days following the statement that Ashley Madison was “offering a \$500,000 reward for information leading to the prosecution of the hackers” (Than Ha, 2015), citing a Toronto Police Acting Staff Superintendent. The utilization of the ‘scapegoat strategy’ became most apparent throughout Ashley Madison’s limited public facing communication - most notably through their consistent messaging and painting of The Impact Team as the party at fault and to blame.

5.3 The Post Crisis Stage

The final stage of findings includes an analysis of the post crisis stage which according to Coombs, should involve “evaluating crisis management, learning from the crisis; and other post crisis actions such as follow up communication with stakeholders and continued monitoring of issues related to the crisis” (2007). While containment and recovery are intrinsic to crisis management, Coombs and Holladay state the importance of post-crisis communication as it “can be used to repair the reputation and/or prevent any further reputational damage” (2005). On July 5, 2016 – one year following the hack – Ashley Madison released a formal statement addressing the hack and steps they had taken throughout the year and would be taking moving forward. It is important to note that no formal press releases related to the hack are visible online beyond the initial response analyzed and few pieces of commentary in news articles on the hack up until this point. This press release will be analyzed in relation to Coombs SCCT in order to determine what and/or if post-crisis actions were employed by Ashley Madison, in addition to Benoit’s Image Repair Strategies considered for their ability to “reduce the perceived offensiveness of the act” (Benoit, 2014). Below is Ashley Madison’s press release, one year post-crisis.






Table 6. Press Release - One Year Post-Crisis Event




Policy & Public Interest

People & Culture

Avid Life Media Breaks Its Silence - Announces New CEO & President - New Leadership and Vision Set to Transform Ashley Madison

NEWS PROVIDED BY
Avid Life Media →
Jul 05, 2016, 07:22 ET

SHARE THIS ARTICLE




TORONTO, July 5, 2016 /CNW/- Almost a year after a criminal hack, Avid Life Media, the company that owns and operates Ashley Madison and other online dating brands, is breaking its silence with the news it has appointed a new CEO and President to lead the company.

Newly appointed CEO Rob Segal and newly appointed President James Millership are three months into their new roles at Avid Life Media and the duo have transformative changes planned for the company and its flagship brand Ashley Madison.

In its first public communication since Segal and Millership took over, Avid Life Media is sharing a social media and radio message with its members – and has announced a new direction and total repositioning of all its brands.

"A year ago, Avid Life Media was silenced by a devastating, criminal hack that affected our company and some of our members. The company is truly sorry for how people's lives and relationships may have been affected by the criminal theft of personal information. That's why we're charting a new course and making some big changes," says Segal.

"Like all businesses in today's security reality, Avid Life Media has been investing even more heavily in security enhancements and privacy safeguards to deal with evolving cyber threats over the past year, and that will continue," he adds. Following the criminal hack on the company, Segal says Avid Life Media partnered with Deloitte's cyber security team, one of the world's leading integrated cyber risk management consultants, to implement new and enhanced security safeguards and 24/7 monitoring. The company is also introducing new, secure and discreet payment options.

"Our new team is committed to taking care of our members and to building on our portfolio of unique and open-minded online dating brands," says Millership, who confirms a total business transformation and rebranding is in the works for Avid Life Media, Ashley Madison and all the company's brands. "Millions of people have continued to connect on our sites during the past year and they deserve a discreet, open-minded community where they can connect with like-minded individuals," he says.

Due Diligence Journey

Both Segal and Millership were carefully selected for their unique leadership abilities: Segal for his marketing and communications leadership; and, Millership for his operational and repositioning experience. Millership and Segal each bring more than 20 years' experience in helping companies reposition, evolve and grow.

New Leadership & Vision Set to Transform Ashley Madison

When they first were presented with the opportunity to lead Avid Life Media, Segal says they were intrigued enough to embark on an extensive due diligence process.

"We talked about how we could help modernize Ashley Madison with a more open-minded, adventurous spirit," recalls Segal. "Soon we were deep into a few months of due diligence to discover what challenges the company was facing and if the fundamentals were in place to allow the company to evolve and grow," he says.

During their due diligence process, the Board mandated a team of independent forensic accounting investigators to review past business practices around bots and the ratio of male and female US members who were active on the site.

The investigation confirmed for Segal and Millership that bots were no longer in use and verified the authenticity of female members. "My understanding is that bots are widespread in the industry, but they are no longer being used, and will not be used, at Avid Life Media and Ashley Madison," says Millership. The independent report confirms that the company discontinued the practise in North America in 2014 and internationally in 2015, he explains.

Building the World's Most Open-Minded Dating Community

"Thousands of new members join Ashley Madison every day from all around the world," says Millership.

"With the right investment, innovation and customer care, the brand has promising potential to overcome its current challenges," he says.

During the post-crisis stage, Coombs noted it is imperative for the organization to continue regular operations; however, so too should they remain cognizant of the potential risk of a future, similar crisis (Coombs 2007). In addition, the company must work towards the continued implementation of image repair plans, regardless of the initial crisis event and 'crisis containment' stage residing. During the post-crisis stage, Coombs outlines three central tasks that an organization should strive to achieve:

1. "Make necessary preparations for similar crises in the future";

2. “Ensure the organization's stakeholders have a positive impression of the crisis management action of the organization after the crisis event”; and
3. “Ensure the crisis has completely ended” (Coombs, 2007).

By accomplishing these three central tasks, an organization can effectively benchmark success and strengthen their overall crisis management and recovery abilities. While the third task is difficult to apply in detail to the above press release, the first and second tasks will be discussed in relation to the communication tactics used to analyze Ashley Madison’s post-crisis stage.

1. Making “necessary preparations for similar crises”

One year following the initial crisis event, Ashley Madison discussed their comeback from the data breach in that they were “charting a new course”, and “making some big changes” (Avid Life Media, 2016). Ashley Madison’s newly appointed CEO, Rob Segal stated continuously how throughout the year, Ashley Madison had been “investing even more heavily in security enhancements and privacy safeguards to deal with evolving cyber threats” and assured that these efforts would continue (2016). In addition, the company discussed their new partnership with a cyber security team at management consulting firm Deloitte, describing them as “one of the world's leading integrated cyber risk management consultants” capable of implementing “new and enhanced security safeguards and 24/7 monitoring” (2016). Lastly, the press release stated they would be introducing “new, secure and discreet payment options” (2016) to reassure users of their utmost priority to keep user-privacy at the forefront of their operations. These steps communicated by Ashley Madison demonstrated a concerted effort to implement change and prepare for similar crises that could potentially occur in the future.

2. Ensuring organization’s stakeholders “have a positive impression of the crisis management action”

Ashley Madison's press release discussed the steps they took to veer away from negative perceptions that continued one year post-crisis. By transparently discussing their efforts to remedy the security issue, Ashley Madison took important steps to acknowledge blame in an effort to begin to shift negative stakeholder perception about the brand. In their press release one year post-crisis event, Ashley Madison utilized the guiding narrative of how their new management took over and successfully reorganized the company in order to repair damage experienced from the hack. This effort to restore public perception became clear as the CEO and President's stated goal was to "rebuild Ashley Madison as the world's most open-minded dating community" through "investing heavily in technology" and by "looking at acquisitions, a total rebranding, new features, partnerships and new ventures" (2016). In addition, the new leader said they were continuing the process of an intense due diligence project aiming to "discover what challenges the company was facing and if the fundamentals were in place to allow the company to evolve and grow" (2016). Throughout this process, the press release further noted Ashley Madison's Board of Directors "mandated a team of independent forensic accounting investigators to review past business practices around bots and the ratio of male and female US members who were active on the site" (2016).

Image Repair and Rebranding After a Crisis

This part of the analysis will apply Benoit's image repair strategies to Ashley Madison's press release one year post-crisis to determine if and/or how their communications sought to reduce any 'perceived offensiveness' of the event. Findings revealed that while Ashley Madison's messaging exemplified defensive tactics, a much greater level of remorse for their victims of the breach were communicated one year post-crisis. The two central strategies by Benoit analyzed were: reducing offensiveness and mortification.

1. Reduce offensiveness

The ‘reduce offensiveness’ strategy was utilized primarily through the following key tactics: transcendence, minimization and attacking the accuser (Benoit, 2016) and are detailed below.

- **Transcendence** – The press release utilized the transcendence strategy by highlighting the company’s pivotal move in hiring a new CEO and President in an effort to transform the company for a better future. The ambitious press release noted that only three months “into their new roles, the duo [had] transformative changes planned for the company and its flagship brand Ashley Madison” (Avid Life Media, 2016). Transcendence was a key message within the press release as it sought to evoke a sense of promise and fundamental change, by articulating past improvement that the company was already undergoing.
- **Minimization** – Ashley Madison utilized the minimization tactic in their press release when reiterating the prevalence of security issues that exist across all lines of business. In doing so, Ashley Madison curtailed focus from themselves and instead highlighted how widespread among companies worldwide that this issue was. Specifically, the press release noted how “like all businesses in today’s security reality,” Ashley Madison had been “investing more heavily in security enhancements and privacy safeguards” (2016). By reiterating how “all businesses in today’s security reality” face similar issues, Ashley Madison reminded the audience they were not the *only* victim to security breaches, effectively minimizing the blame on themselves, whilst offering a reminder of the steps that they were taking nonetheless.
- **Attack accuser** – Ashley Madison employed the tactic of attacking the accuser by weaving in how this was a “criminal” act experienced throughout their communication.

The release noted how their consumers had been “affected by the *criminal* theft” and that “following the *criminal* hack”, the company partnered with a cyber risk management consultant to reincorporate effective security measures.

2. Mortification

An application of Benoit’s second image repair strategy, ‘mortification’, was conducted by deconstructing Ashley Madison’s apology and determining whether the statement embodied the tactic. Ashley Madison noted in 2015 that they were “silenced by a devastating, criminal hack that affected [their] company and some of [their] members”, and were “truly sorry for how people's lives may have been affected by the criminal theft” (Avid Life Media, 2016). While Ashley Madison’s apology exemplified a level of regret for the damage the crisis induced, Benoit’s *minimization* tactic was deftly woven within their language, ultimately rendering their apology trivial. When stating their apology to parties that “may have been affected by the criminal theft”, Ashley Madison failed to address those *knowingly* affected by the crisis – i.e., those reported to have committed suicide, faced divorce, lost their jobs and those whose reputations were compromised by their private information being made public. In addition, by communicating their apology in direct relation to the “criminal theft” experienced, Ashley Madison devalued their level of sincere ‘mortification’ regarding the crisis. Similar to their communication during the crisis event stage, Ashley Madison failed to properly execute Benoit’s mortification strategy in that they did not ask for forgiveness nor take full responsibility for what happened.

With image repair theory, Benoit argued that one’s beliefs often coincide with their values in order to form a particular attitude; as such, different audience members “can (and usually do) have a variety of belief/value pairs” (2015) when it comes to public perceptions of a

crisis event. To exemplify this notion, Benoit stated that while one person may consider former U.S. President Bill Clinton highly respectable solely due to his status and operations, others might view him in a very unfavourable light as a result of his admitted marital affair (2015) and ensuing impeachment. This example is particularly compelling when considering the differing viewpoints and “truths” a stakeholder and/or consumer may hold about a company such as Ashley Madison during the crisis at hand. More specifically, Benoit argues that “perceptions are more important than reality”, in that the most important factor is not “whether the business is responsible for the offensive act”, but rather, if the firm is “thought to be responsible for it by the relevant audience” (1997). While Ashley Madison consistently deemed The Impact Team as criminals – for illegally hacking into their software and extorting them – The Impact Team’s motives for expunging the site due to illicit security measures and immoral business practices remained the common narrative within the news and social media. In addition, Ashley Madison was commonly touted for “misrepresent[ing] how secure [their] site was, [and caused] “substantial consumer harm” by failing to take reasonable steps to prevent unauthorized access by hackers” (Kuchler, 2016). The previous application of Coombs’ SCCT validated many missteps/faults within not only Ashley Madison’s crisis communication but their internal security software, however, Benoit makes the important distinction within IRT that persuasive attacks – which include the “attempt to create (or strengthen) a negative attitude toward a target” (2015) – often take place and can augment people’s perceived reality.

As such, it becomes clear that few audiences and perceptions around the Ashley Madison crisis persisted - including The Impact Team’s perception that the company exhibited corrupt security measures and is fundamentally immoral. Certain news outlets expressed support for The Impact Team’s effort to expunge the site for providing an “immoral service”, while a limited

number of others called for the prosecution of The Impact Team for their illegal hack and proliferation of private information. However, throughout the press releases and public facing communication, Ashley Madison made no effort to communicate or address competing audiences. Instead, the company released sparse amounts of communication, addressing the hack as criminal and themselves as victims. Reports from the privacy commissioner proved that despite Ashley Madison's claims that they had remedied the issue throughout the initial crisis event, the company indeed lacked proper security measures and failed to protect and communicate with their valued customers.

Discussion

Similar to how an “airline should anticipate the possibility of a crash” and “a restaurant should prepare for cases of food-poisoning” (Benoit, 1997), a discreet online dating company should anticipate a data breach. While Ashley Madison demonstrated irresponsible security measures and a lack of strong, ongoing crisis communication to their stakeholders throughout the crisis, it is important to consider this crisis and its relationship to the reputation Ashley Madison had prior to its occurrence. SCCT allows for the crisis manager to deconstruct their response strategies through the way stakeholders might understand and best receive the crisis, however, it is additionally significant to discuss Coombs' theory of the velcro and halo effects for companies that might face either increased or decreased reputational threat due to prior reputational values held about them. Coombs validated these theories when stating that “the history and prior reputation of a company is essential when assessing the reputational threat of a crisis”, and thus which image repair strategy the company should choose to employ (2007). The first notion of the ‘velcro effect’ quite literally leverages the idea of velcro attracting lint, in that an organization

with a history of crises or poor reputation will likely attract additional reputational threat (Coombs, 2006). Coombs added that this threat can take place not only in terms of crises, but also reputation (2006). Specifically, a company with a negative prior reputation has a heightened risk of further tarnishing their current reputation once a crisis takes place, meaning the crisis is not to be considered an “isolated event” but rather part of a larger “pattern of organizational performance” (Coombs, 2010). This effect holds particular significance with companies such as Ashley Madison who have faced controversial reputations in the past – for monetizing the facilitation of extramarital affairs from the outset of their business, and upon the data breach faced, for being a renegade in the information security community.

While it was beyond the scope of this MRP to provide a deep analysis of stakeholder perceptions, it is clear Ashley Madison had a controversial reputation from the outset. Ashley Madison’s heightened difficulty due to its negative prior reputation is supported by Coombs and Holladay’s assertion that “a favourable prior reputation protects the organization’s reputation from the increased threat of a ‘human error crisis’” whereas “an unfavourable prior reputation automatically makes a ‘technical error crisis’ appear like a ‘human error crisis’”— thus intensifying the reputational threat (2010). While it is clear the data breach was not Ashley Madison’s intent, the organization faced immense scrutiny for having prided themselves on secrecy when ironically, their software lacked the advanced security and reliable protection that its customers expected. Moreover, as the prior reputation of secrecy and infidelity caused additional reputational threat to Ashley Madison from the outset, the response strategies executed ultimately still perpetuated the company’s poor reputation.

Ahead of applying crisis response strategies to this case study, it was imperative to first consider a set of guidelines for how an organization should properly utilize them. As such, the

first consideration was to determine if Ashley Madison's initial response adhered to Coombs' guidelines for 'instructing and informing information'. Next, an analysis of the crisis situation and 'basic crisis response options' took place, knowing that "crisis managers can choose which, if any, to use in a crisis situation," and how it is more about selecting the most *appropriate* strategies (Coombs, 2006) based on the crisis situation. First, Ashley Madison provided limited 'informing and adjusting information' throughout the initial crisis event and month following which was revealed to be a significantly poor approach as the company had a high attribution of crisis responsibility based on the situation at hand. Throughout the crisis, Ashley Madison continued to communicate from a "victim crisis" perspective – never assuming or taking full blame for the situation despite having been proved responsible for lack of security. In addition, Coombs suggests that "diminish crisis response strategies should be used for crises with low attributions of crisis responsibility" (2007), meanwhile, this strategy was apparent within their initial press release. Further, 'rebuild crisis response strategies' were not employed during the timeframe analyzed; instead, Ashley Madison remained inconspicuous in their public communications and failed to address their consumers during the evolution of events and data released from The Impact Team. Given Ashley Madison's high attribution of crisis responsibility, rebuild strategies should have been at the forefront of the company's crisis response. However, the company failed to match their reputation to the threat of the situation and effectively convey messages to their stakeholders. By failing to advise stakeholders/consumers how to "protect themselves from the crisis" (instructing information) and provide insight as to coping with emotional and psychological issues resulting from the crisis (adjusting information) in a consistent, dedicated manner, Ashley Madison inadequately met Coombs guidelines for crisis response strategies.

In aggregating the 10 SCCT crisis response strategies, Ashley Madison most notably employed five approaches throughout the public responses analyzed. These strategies were: scapegoat/victimage, attack accuser, excuse, justification and ingratiation. However, given the high level of responsibility attributed to Ashley Madison for the crisis, it can be concluded that the company's most utilized approaches failed to meet Coombs' suggestion that "the more responsibility stakeholders attribute to the organization, the more the crisis response strategy must seem to accept responsibility for the crisis" (Coombs, 2006). Of the five most leveraged response strategies, not one sought to properly deal with the crisis at hand - through strategies such as: providing a sincere apology, express concern for victims of the crisis, offer direct compensation to consumers or demonstrate a high level of remorse or regret.

In addition, Ashley Madison failed to adhere to the following guidelines that: 1) the *deny* crisis response strategies should be used for rumour and challenge crises, when possible and 2) organizations must maintain consistency in crisis response strategies. Upon analysis, it is clear that the Ashley Madison data breach was indeed a preventable crisis, and the resulting damage was exacerbated by the organization's unrepentant denial of responsibility in the hack from its inception. Further, the lack of consistency and timeliness in messaging greatly hindered their ability to maintain a strong, level-headed approach to adequately handle the crisis.

Conclusion

While Ashley Madison faced immense casualties from the 2015 data breach, it might be surprising to readers how in 2019, Forbes reported the company to have "amassed around 32 million new users since the hack" (Doffman, 2019). Specifically, Chief Strategy Officer at Ashley Madison Paul Keable, provided that before the 2015 events, the company garnered

approximately 30,000 new members daily and now, they're "back [up] to around 22,000" (Doffman, 2019). Keable also acknowledged their damaged reputation due to the hack, stating how they "needed to tell people where [they] stood in a way they could trust" and that in 2018, they leveraged Ernst and Young to verify their security and sift through "all [of their] systems, inch by inch", confirm that all fake-female profiles were obsolete and instilled a "sense of purpose for security" (Doffman, 2019). When speaking to how the "wholesale leaking of private data" would be thought of as existential to a company's trajectory, Keable provided that "the easy-to-navigate extra-marital affair" their service provides "is simply too enticing to avoid" (Doffman, 2019). However, can the comeback and current success of the company be attributed to their crisis management operations? When asked about lessons learned from the crisis and what the Chief Security Officer thought should have been done differently looking back, Keable replied solely with having "better security" (Doffman, 2019). However, this MRP utilized textual content analysis to deconstruct Ashley Madison's communications to determine the success and appropriateness of their crisis communication strategy. In maintaining and employing SCCT as the primary framework for analysis, findings proved that Ashley Madison failed to properly communicate the truth that they had inappropriate internal safeguards and security frameworks that allowed the crisis to forge when confronted by attacking hackers. While difficult to determine all facets of communication from each stakeholder, particularly due to the scope of this MRP, the research conducted determined many faults and discrepancies within Ashley Madison's crisis response, despite the Chief Strategy Officer's perception that their only pitfall was a lack of security.

While Ashley Madison's lack of proper security measures ultimately rendered the crisis as preventable on their part, it is of further research interest to consider what ramifications hacker

groups might face (such as The Impact Team - who remain anonymous to this day) – when crossing the virtual borders of a company’s private user information. This brings into question The Impact Team’s goal of exposing Ashley Madison’s lack of software security and unethical business activities, challenging whether the cost of innocent user information being exposed and personal lives compromised is worth the divulgence of organizational flaws. Despite further exploration required to address the morality of The Impact’s Team’s hack, the notwithstanding fundamental flaw in Ashley Madison’s crisis communication strategy was their lack of properly assessing attribution of responsibility. Ashley Madison consistently played the role of the victim by communicating that the breach was not their fault and that they were targets of a criminal act. This unclaimed responsibility left consumers helpless, absent of any knowledge related to Ashley Madison’s plan to take responsibility for and rectify the crisis at hand. Despite Ashley Madison being significantly implicated as a company, the crisis directly impacted more than 37 million users – leading to many consumer casualties including suicide, divorce and permanent individual reputational damage (Adophia, 2015). Given the extremity of the crisis and the populational range of its result, Ashley Madison failed to meet its fiduciary duty of communicating responsibility and honesty to their users, effectively leaving them unprotected from further reputational damage.

This case study proved that from the outset, Ashley Madison should have placed their customers at the forefront to safeguard their future reputation as well as reinforce the trust and value required from their primary stakeholders. Based on the literature review and Coombs’ SCCT, findings revealed several weaknesses in Ashley Madison’s crisis communication response. In turn, this led to more problems for the company. This case study highlighted the need for organizations to employ proper, situationally-sound strategies that place immediacy,

ongoing communication and transparency at the forefront. While Coombs posits stakeholders and the news media require and expect immediate responses from organizations (2007), this MRP revealed that a much more sophisticated and strategic degree of messaging by a company involved in a crisis is not only beneficial, but vital.

References

- Adophia, V. (2015, August 20). Sources confirm hacked Ashley Madison data is authentic | CBC News. Retrieved from <https://www.cbc.ca/news/canada/toronto/ashley-madison-data-1.3196636>
- Arnett, R., Deiuliis, S. & Corr, M. (2017). *Corporate communication crisis leadership: advocacy and ethics*. Business Expert Press.
- Benoit, W. (2014): Accounts, excuses, and apologies: A theory of image restoration strategies. State University of New York Press.
- Benoit, W. L. (1997). Image repair discourse and crisis communication. *Public Relations Review*, 23(2), 177-186. doi:10.1016/s0363-8111(97)90023-0
- Benoit, W. L. (1995). Sears' repair of its auto service image: Image restoration discourse in the corporate sector. *Communication Studies*, 46(1-2), 89-105. Retrieved from <http://ezproxy.lib.ryerson.ca/login?url=https://search-proquest-com.ezproxy.lib.ryerson.ca/docview/233197484?accountid=13631>
- Carroll, C. (2009): "Defying a Reputational Crisis - Cadbury's Salmonella Scare: Why Are Customers Willing to Forgive and Forget?" *Corporate Reputation Review*, 12(1), 64-82
- Coombs, W. T. (2006). The Protective Powers of Crisis Response Strategies. *Journal of Promotion Management*, 12(3-4), 241-260. doi:10.1300/j057v12n03_13
- 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:10.1057/palgrave.crr.1550049
- Coombs, W. T., & Holladay, S. J. (2010). *The handbook of crisis communication*. Chichester, West Sussex: John Wiley & Sons.
- Doffman, Z. (2019, August 27). Ashley Madison Has Signed 30 Million Cheating Spouses. Again. Has Anything Changed? Retrieved from <https://www.forbes.com/sites/zakdoffman/2019/08/23/ashley-madison-is-back-with-30-illion-cheating-spouses-signed-since-the-hack/#680089a38787>
- Frandsen, F., & Johansen, W. (2017). *Organizational Crisis Communication*. SAGE Publications, 70-87.

- Johnson, D., & Sellnow, T. (1995). Deliberative rhetoric as a step in organizational crisis management: Exxon as a case study. *Communication Reports*, 8(1), 54–60. doi: 10.1080/08934219509367607
- Jordan, T., & Taylor, P. A. (2004). *Hactivism and cyberwars: Rebels with a cause?* New York, NY: Routledge.
- Koerber, D. (2017). *Crisis Communication in Canada*. University of Toronto Press.
- Kuchler, H. (2016, December 14). Ashley Madison agrees to \$1.6m fine for data breach. Retrieved from <https://www-ft-com.ezproxy.babson.edu/content/db7a5c42-c21a-11e6-9bca-2b93a6856354>
- Krebs, B. (2015, July 15). Online Cheating Site AshleyMadison Hacked. Retrieved from <https://krebsonsecurity.com/2015/07/online-cheating-site-ashleymadison-hacked/>
- Lamont, T. (2016, February 28). Life after the Ashley Madison affair. Retrieved from <https://www.theguardian.com/technology/2016/feb/28/what-happened-after-ashley-madison-was-hacked>
- Lord, N. (2017, July 27). A Timeline of the Ashley Madison Hack. Retrieved from <https://digitalguardian.com/blog/timeline-ashley-madison-hack>
- Office of the Privacy Commissioner of Canada. (2016, August 23). PIPEDA Report of Findings #2016-005: Joint investigation of Ashley Madison by the Privacy Commissioner of Canada and the Australian Privacy Commissioner/Acting Australian Information Commissioner. Retrieved from <https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2016/pipeda-2016-005/#c5>
- Scheurman, G., & Evans, R. W. (2018). *Constructivism and the new social studies: A collection of classic inquiry lessons*. Charlotte, NC: Information Age Publishing.
- Schwarz, A., Seeger, M. W., & Auer, C. (2016). *The handbook of international crisis communication research*. Southern Gate, Chichester, West Sussex, UK: Wiley Blackwell.
- Schwartz, D. (2015, August 26). Ashley Madison hackers could face long list of charges | CBC News. Retrieved from <https://www.cbc.ca/news/technology/ashley-madison-hackers-impact-team-could-face-long-list-of-charges-1.3203279>
- Smith, D. and Elliot, D. (2006). Key readings in crisis management. New York: Routledge.
- Sorensen July 20, C. (2015, July 21). Ashley Madison's Achilles heel is exposed, and it's not morality. Retrieved from <https://www.macleans.ca/economy/ashley-madisons-achilles-heel-is-exposed-and-its-not-immorality/>

Syed, F., Cribb, R., & And, F. S. (2018, March 29). Another date for Ashley Madison? Retrieved from <https://www.thestar.com/business/2018/03/29/another-date-for-ashley-madison.html>

Tuttle, H. (2015). Implications of the Ashley Madison hack. *Risk Management*, 62(8), 6.

Ulmer, R. R., Sellnow, T. L., & Seeger, M. W. (2019). *Effective crisis communication moving from crisis to opportunity*. Los Angeles: SAGE.

Ward, M. (2015, August 20). Ashley Madison: Who are the hackers behind the attack? Retrieved from <https://www.bbc.com/news/technology-34002053>

Zaremba, A. J. (2015). *Crisis communication: Theory and practice*.