Journal of Risk Analysis and Crisis Response, Vol. 4, No. 3 (September 2014), 151-159

A Gamer's Nightmare: An Analysis of the Sony PlayStation Hacking Crisis

Bolanle A. Olaniran

Department of Communication Studies, Texas Tech University, P. O. Box 43083
Lubbock, Texas 79409-3083, USA
E-mail:B.Olaniran@ttu.edu

Andrew Potter

Department of Communication Studies, Texas Tech University, P. O. Box 43083
Lubbock, Texas 79409-3083, USA

Katy A. Ross
Department of Communication Studies, Texas Tech University, P. O. Box 43083
Lubbock, Texas 79409-3083, USA

Brad Johnson
Department of Communication Studies, Texas Tech University, P. O. Box 43083
Lubbock, Texas 79409-3083, USA

Received 7 May 2014

Accepted 30 July 2014

Abstract

The Sony PlayStation hacking crisis presents all too common personal data theft in the digital information age. The hacking necessitates the need for how such a crisis could be prevented in an attempt to safeguard customers' personal information and ensure trust between client and vendor relationship. The research focuses on assessment of the Sony PlayStation hacking using the Anticipatory Model of Crisis Management (AMCM). Using the AMCM principles, it was found that Sony Corporation could have handled the crisis better.

Keywords: Crisis management, Crisis preparedness, Anticipatory model, Hacking.

1. Introduction and Rationale

Organizations inevitably experience crisis and whether or not the organization is prepared for a crisis determines some of the extent of the crisis at hand. Scholars argue that a model is needed in order to help stop crises before they arise prompting the creation of the Anticipatory Model of Crisis Management. Sony's crisis in April of 2011 provides a significant example for studying the effects of an organization's crisis to understand better the implications of taking certain actions to alleviate a crisis. Sony experienced a security breach of its online service called the PlayStation Network, and millions of customers had personal information stolen including credit card information. Sony estimates the losses from the PlayStation Network hacked at $171 million[1]. The purpose of this paper is to explore Sony's crisis through a framework of the Anticipatory Model of Crisis Management to highlight

important implications for online service providers in the future.

2. Case Overview

Sony Corporation is a company that produces several electronics. One of the more popular products produced by Sony is the PlayStation gaming system. Sony found itself in a colossal security breach. On April 20, 2011, Sony executives started to investigate abnormal activity on the PlayStation network, which ultimately led to the theft of over 100 million PlayStation users' personal information and for some, credit card information[2-4]. Sony shut down the network the day after suspicious activity was detected and although Sony released almost daily announcements concerning the system outage, the company waited almost a week (i.e., six days) after initial recognition to release an announcement of the hacking itself [3, 5-6]. In the final analysis, Sony is reported to have invested approximately $170 million to cover the expenses of caring for the consumers that had been affected, improving the network's security and customer support, as well as the investigation into the hacking[4]. The next portion of this case study offers a brief overview of the anticipatory model of crisis management, which is used to examine the effectiveness of Sony's handling of the PlayStation hacking case.

3. Anticipatory Model of Crisis Management

Organizational crisis is defined as an unpredictable or a major threat that could have a negative effect on the credibility of the organization, the industry or its stakeholders[7-9]. In essence, crisis is characterize as an event that compromises one's safety, customers, community, or threatens to destroy public trust in the organization, thus, damaging the company's reputation[10]. Hence an effective crisis management embodies a proactive approach that include prevention and especially at the pre-crisis phase[7, 11-13]. Therefore, the anticipatory model of crisis management was created to meet this need.

The anticipatory model of crisis management, otherwise referred to as the AMCM, was originally developed to address crisis and crisis management at the front end rather than after the fact. The AMCM contends that while one might not be able to prevent all crises from occurring, emphasis on preventing crisis from happening should still be a major priority. The central position of the anticipatory model is that significant attempts ought to be made to put in place programs that assess possible crisis triggering factors, such as human error and natural disaster among others, while putting in place appropriate plans to handle any crisis if and when they do occur. The original formulation of AMCM was initially designed to address crisis emanating from organizational use of technology[12]. However, the AMCM has been extended to other forms of crisis beyond technology and the new anticipatory orientation toward crisis management has moved the starting point for crisis evaluation[13]. The definition of crisis reflects the sense that the prevention of crisis not only safeguards the public's health and safety, but also preserves the trust that the public has for organizations to prevent crises by ensuring their products are safe and that their business practices and communication with the public are honest while demonstrating good citizenry in the community in which these organizations exist or operate. With regard to public safety, the anticipatory model implies that best practices are maintained through competent communication within the organization and with the public as a whole.

The basic premises and assumptions of the AMCM consist of three main factors, namely expectations, enactment, and control. The expectation principle, speaks to the assumptions that people make about certain events[12, 14-16.] For example, expectations about the likelihood of a crisis happening would determine whether or not one made the provision to put in place a preventive action or countermeasure. However, it stands to reason that assumptions via expectation have the potential to bring about a self-fulfilling prophecy. For example, when organizational decision-makers assume that a particular technology is fail-safe, they err and might relax safety mechanisms and measures, such that additional counter measures become an afterthought and are never put in place to create necessary a buffer or redundant procedures [12, 14-17.]

Regarding enactment, the assumption is that the very action that enables people and organizations can also cause destruction[18]. This idea pertains to the principles of enactment and expectations, which are germane to the anticipatory model[12-15]. Enactment focuses on a process where a given action is brought about[19]. The notion of enactment was eventually extended to

consequences from those actions[18]. For example, failure to put in place a crisis plan might negatively impact the eventual or ensuing crisis management. With enactment conceived as a retrospective sense-making process, the model contends that the notion of "anticipation" (of crisis) in and of itself is an action, given that it determines the subsequent choices an organization makes based on available information. There is justification for this claim given the fact that decision-makers and especially organizational leaders often find themselves in situations where they have to envision opportunities, threats, and weaknesses in their environment and then take appropriate measures to safeguard their interests. Therefore, the model asserts that decision-makers' actions or inactions with anticipation would result in different outcomes.

The third element in the model is the idea of control, which is the degree of power an organization has over events or crises. For example, if it is discovered that a shipment of medicine leaving a factory is tainted or deficient in anyway, control might refer to the company's ability to stop the shipment before it hits pharmacy shelves. The control component intertwines with expectation and enactment to the extent that expectations influence enactments (decisions or actions) and actions exerts control over crisis situations. The same can be said for all the three major components of AMCM that they are hierarchical rather than mutually exclusive. In essence, the model is complex rather than linear and takes into consideration that all the three components are intertwined and interdependent.

In sum, crisis prevention requires a thorough reconnaissance of the complexity of relationships within (internal) and their environmental contexts (external). Nevertheless, enactment and expectation must be present to facilitate an understanding of the process [12, 18]. While enactment consists of specific actions, expectation about an object determines the type of action taken in the enactment process and provides organizations the needed control to handle a crisis. Taken together these factors constitute the anticipatory process of crisis planning and crisis aftermath— where the occurrence of a crisis is foreseen and effort is made to avert or at minimum, reduce the impact of the catastrophe. As part of crisis planning and prevention, the issues management perspective and other crisis management literature have acknowledged the usefulness of AMCM as a valuable tool in the crisis literature[20-21]. Furthermore, beside AMCM usage as an organizational communication tool in gaining and maintaining the public trust, it also serves as a key reminder that crisis prevention is critical and can make the difference in a matter of life and death for community members and other stakeholders. In the next section, the methods of this study are divulged.

4. Methods

In crisis management research, a common method used is case study. This project used a case study focusing on Sony PlayStation. The researchers utilized and examined accessible news materials from media channels including news reports and stories. The news materials are analyzed in an attempt to track the chain of events in the issue of the Sony PlayStation hacking crisis. The researchers used the tenets of the AMCM model to assess decisions Sony made during the course of the crisis. Case studies involve the process of analyzing in depth, a particular event or phenomenon, such as the Sony crisis, by examining detailed information surrounding the event[22-24]. The goals of this study were to uncover the exact missteps Sony made in managing its crisis. Thus, the series of decisions in the Sony PlayStation hacking case were arranged on a timeline to better explore the case in its entirety. A timeline arrangement aids the researchers in tracking the steps and narrowing down the areas in which the organization made mistakes.

Additionally, the timeline technique affords a methodological approach that utilizes assumptions and ideas of the anticipatory model of crisis management (AMCM), which were used to investigate and assess Sony's PlayStation hacking crisis communication and management. Therefore, the study analyzed and evaluated accessible news materials through the lens of AMCM. From the analysis, implications and limitations of the case study were offered. The following section provides an evaluation of the Sony PlayStation hacking crisis.

5. Analysis and Evaluation of Sony PlayStation Hacking Case

There are four separate instances of how the tenets of the AMCM apply to the ways in which Sony handled the situation of the PlayStation Network intrusion. First, Sony failed to inform their customers about the breach until a week after the hackers infiltrated the network.

Also, Sony failed to inform the customers that credit card information have been stolen or compromised. Instead, Sony said that they did not believe financial information was stolen. Second, Sony did not immediately shut down the network when it knew of a possible security breach. Third, Sony inaccurately accused a hacker group without the proper information. Fourth, Sony gave a timeline for the network to be fully functional again, which it did not meet. All four of these components of the network crisis provide ample information for organizations to prepare better if they learn through the AMCM.

Enactment and expectations all enlighten the first aspect of the Sony PlayStation hacking crisis. Expectations play a huge role in the first element of the Sony crisis because consumers expect corporations to safeguard their credit card information when consumers are purchasing a product. However, Sony did not meet the expectation principle because the credit card information was stolen from 12 million of the members[2] and the hackers threatened to sell the information. Expectation was also not met concerning the security breach because Sony did not immediately inform its consumers that a security breach had occurred. Sony waited one week after the initial breach to inform anyone outside of the organization about the breach. Once it was known that the hackers stole credit card information during the breach, it means that there was an entire week where the information of millions of customers was in the hands of hackers and the consumers could not protect themselves. Similar to the previous point, consumers expect a notification if there is even the slightest possibility their confidential information could be at risk. Consumers' expectations were not met when Sony did not act immediately and prudently on the information it possesses.

Sony left the Sony PlayStation network up and running while the crisis was ongoing, which affects all of the aspects of the AMCM. Sony had the control to make sure the security was the best available, consumers expect the best security, and Sony could not act because of the lack of security measures, so all aspects of the AMCM are present when evaluating Sony's lapse of action. Similar to how Sony did not inform players of the network being hacked, Sony did not immediately close the network when the breach occurred because Sony's security could not detect the intrusion was occurring. Sony waited until April 20th before acting on the information about network intrusion[25]. Although, a company may be strategic in not alarming the public, but recent crises has shown for the most part that such a lack of notification is nothing more than mere incompetence[26-27]. Furthermore, if Sony had shut down the network immediately on the 17th, then few information would have been stolen by the hackers. The notification, would have also given affected customers the opportunity to take certain actions on their own (e.g., canceling credit cards). Sony's inability to act effectively affects both control of the crisis and expectations discussed in the AMCM. Consumers expect that a company would take all measures to stop a crisis from spiraling out of control. If the network was hacked, then consumers would expect Sony to close any other possible ways the hackers could affect the network, which would probably entail shutting down the network. Sony has direct control on whether or not the PlayStation Network functions or not because Sony owns the network. Failing to act in a manner that is completely within a company's direct control violates the vigilance test of the AMCM.

The notion of control also highlights an aspect of the crisis where consumer expectations were not met at the pre-crisis stage. Sony may not be able to control whether or not hackers want to hack into a network. However, Sony can control whether or not it has the best security in place for the network as highlighted by Sony's commitment to increasing security after the breach occurred[25]. Sony's lack of effective detection system compromises the security of the entire system. Hackers continued to attack for three days while Sony was oblivious to the attack. Lulzsec, the group responsible for the intrusion, detailed its intentions for the attack as being simple, stating on June 2nd through a post on *The Pirate Bay*: "Our goal here is not to come across as master hackers, hence what we're about to reveal: SonyPictures.com was owned by a very simple SQL injection, one of the most primitive and common vulnerabilities, as we should all know by now. From a single injection, we accessed EVERYTHING. Why do you put such faith in a company that allows itself to become open to these simple attacks?"[28].

Sony revamped its security scheme after the breach occurred, which implies that additional security existed in the first place[25] but Sony chose not to use the increased security for some reasons. Consumers expect their information to be secure with the best sort of

encryption security especially if the information deals with finances. Sony again violated those expectations by not adequately preparing for a possible crisis, which resulted in its 2011 crisis.

Sony's third issue when using the AMCM was that Sony blamed the hacking group "Anonymous" when the group had nothing to do with the 2011 breach[29]. Instead of investigating the issue completely, Sony decided to initially blame Anonymous without the adequate information. Sony had previously prosecuted George Hotz, an Anonymous hacker, for tampering with the PlayStation 3 to allow it to play unlicensed software, which Hotz proceeded to inform other players how to do the same[29]. Sony assumed and believed without credible information that Anonymous perpetrated the attack because a text file titled "Anonymous" with the contents reading "We are legion," part of Anonymous' motto, was found in the Sony servers after the intrusion. Anonymous denied the claim by issuing the statement on May 4, 2011: "If you think Anonymous placed the 'file' on the PSN try this out. Right click on your desktop, make a new text file, name it anonymous, and type in the text file, 'We are legion.' That done?"[28]. Eventually, Lulzsec, accepted the responsibility for the PlayStation Network intrusion[30]. Sony's false statement implicates the notions of expectations and enactment. Consumers expect that an organization knows what caused a crisis and if the organization does not know, then consumers do not want a corporation that falsely accuses individuals or organizations for the shortcomings of the corporation experiencing a crisis. Falsely accusing Anonymous further hurts Sony's crisis management because it looked as if Sony did not know what was going on, which consumers expect of a multi-billion dollar company. Also, the fact that the crisis was kept secret for a week should have given Sony ample time to investigate the problem. Thus, Sony's behavior and actions did not meet the consumers' expectation that Sony should be able to provide them credible explanation about the crisis and in a timely manner. At the same time, falsely accusing another organization for the problem makes Sony look as if it was not willing to accept its own responsibility for the crisis. Sony tried to pin the crisis on a hacking group, which was fairly well-known, and make the hacking group the scapegoat instead of taking responsibility for how its networks was compromised. The blame shifting and scapegoating strategies by Sony not only violates expectations but also hurts Sony in the eyes of its consumers.

Furthermore, Sony set a timeline to restore the PlayStation Network and did not meet the deadline. Sony vowed to restore the network within a week's time and did not meet its own expectation. First, this hurt the company's consumers because consumers expect a technological company to understand how much work is needed to restore a network. Instead, Sony looked incompetent when it came to knowing how long it would take to restore the network, which did not help Sony's perception immediately after failing to stop a security breach on their network. Second, control was affected by failing to meet the timeline because it is completely within the company's power to meet its own deadlines. Sony initially set the deadline at a week[25], so Sony had control as to when the network needed to be restored because it was Sony, not the media or gamers, who had full control on how to handle consumer expectations. Sony looked as if it did not have any clue regarding the functionality of its network, the security of the network, and capability of its technicians in repairing the network. Subsequently, consumer expectations and hopes were further dashed due to the lack of control demonstrated by Sony. Finally, enacting the decision to restore the network appeared to be the right thing; however, the company should have put in place measures to meet the self-stipulated deadline. Expectations were high and the reestablishing of the network was completely within the control of the company but the slow implementation of necessary protocol to meet the deadline did not bode well and hinders customers and other members of the public's faith in Sony and its crisis management plan. Next, the implications of this case study with AMCM on a general business psychology level are discussed.

6. Implications

Crisis preparation without consideration of shareholder psychology in crisis response can create unintended and potentially costly consequences[31]. Sony, in adhering to a traditional liability-reduction crisis management model, made this error. As a result what could have been a modest corporate public relations challenge evolved into a major company-wide crisis, eventually costing the company hundreds of millions of dollars.

Manufacturers' intensive promotion of internet-based gaming technology has resulted in a gaming community dedicated to cooperative online play (e.g. Call of Duty series, World of Warcraft, etc.). In addition to individual gaming manufacturers' marketing inferences attempting to imply a generally superior technology such as the online gaming community tends to consist of individuals in their late teens to mid-thirties[32]. However, this age range has little tolerance for unreliable technology. Also, these individuals crave uninterrupted online access for a significant part of their social, educational, and/or family interaction regimes[32]. Adding to this is a generally heightened emotional response to perceived injustices, both personal and social. Not considering this volatile mix of dedication, reliance, technological expectation, and emotional reaction into an organization's pre-crisis planning will likely yield catastrophic results.

Adherence to traditional procedure and reactive crisis response will no longer suffice in a world dominated by preference for instant-access to social and informational technologies. Once the product of a simple checklist, crisis handling must now incorporate psychology and a presumption of instant and significant shareholder interaction via any number of electronic and social-media. Corporations and crisis managers must also presume that their shareholder base is literally the entire world. At the very least it will be a significant community of like-minded individuals or entities, which communicate with a rapidity and volume unseen in human history.

One component, which cannot be ignored, is the company's own history and reputation within the industry, customer base, or community-online or otherwise. Sony discovered this when its history became a distinct liability. Its technological prowess and proclaimed commitment to dependability created a presumption of *absolute reliability and trust* in the gaming community. A boon for marketing, sales, and resulting corporate investors along with profitability created a presumption of infallibility and complete trustworthiness among consumers. Nevertheless, when this expectation was challenged, the result was a perceived breach of faith with consumers that ensued immediate and costly backlash within the gaming community.

As seen in the Sony debacle, public relations departments and ample pre-crisis social considerations can play as much, or more, of a part in risk mitigation than an organization's legal department. The shareholder base must not only be advised of actions, they must also perceive a corporate empathy and a sense of the corporation's dedication to affected parties' well-being. Without this, actions shielding the corporation from legal liability on a particular issue will do little to alleviate the expense and public relations issues stemming from a likely flurry of nuisance litigation. Meritless litigation, born of a sense of social justice or righteous indignation no less costly or resource intensive than more substantive legal challenges, and may well prove more expensive in the long-term.

The issue of ongoing consumer and shareholder confidence is of great importance and should be considered a critical part of comprehensive pre-crisis planning. A few minutes on social media sites such as Facebook give graphic illustrations of the tenacity of social memory, correct or otherwise, as it relates to corporate identities. Unrelated issues from years past, sometimes decades, are seen circulating on a perpetual basis. It is common to see issues posted to Facebook as current, vital, and deeply troubling only to be illustrated as revisions of urban legends and society-wide misinterpretations[33]. This is especially true of issues resulting from event associations with a significant customer vesting component, the emotional attachment creating a sense of injustice and giving rise to all manner of misperception and uninformed presumption. The 2011 Sony crisis is a prime example as the online gaming community continues to view Sony as somewhat untrustworthy. Responses from various participants at Sony's online gaming forums[34] indicate that some gamers remain wary of Sony's dedication to both game support and customer confidentiality.

The Sony PlayStation hacking case explicitly demonstrates how issue-based traditional crisis management strategies are no longer sufficient. These strategies presume an event-response relationship; using rigid protocols developed under centralized control structures and with corporate efficiency and liability mitigation the central concerns. This ignores one of the AMCM pre-crisis planning basics, integrating fluidity and flexibility into the crisis response plan. A rigid plan cannot accommodate the randomness and emotional responses of human nature. Thus, response schedules and logistics outside the scope and scale of the pre-planned contingency plan render the plan all but useless.

Given a rigid, centralized organizational philosophy, this resulting chaos can become overwhelming. Notwithstanding, some of these challenges can be mitigated to a great degree by implementing AMCM, using pre-crisis planning as a springboard for planning, testing, and revision in a beta environment. This allows identification and resolution of potential problem areas, including a more thorough training for crisis management teams.

Organizations, in general, can no longer afford traditional crisis planning methods. The traditional methods are inherently flawed when faced with modern technologies and societal expectations. In the age of instant global communication and community interaction via any number of social media outlets, stakeholders form opinions and initiate their responses faster than any traditional corporate crisis plan can accommodate. Without a switch to AMCM prevention centered mode or similar modality, crises that would have been quickly and simply dealt with in years past can, and often will, become insurmountable social and legal burdens. A failure to address human nature, especially in the areas of setting expectations and addressing a desire for regular, relevant information, yields an emotional gap which stakeholders will rush to fill with their own perceptions, presumptions, and conclusions, and which they then immediately begin communicating or sharing with others. The more emotional the stakeholder investment, the faster the information spreads. A popular idea, benevolent or otherwise, can grow to global scale in a matter of hours.

This sea of social activity inevitably spawns issues which, regardless of accuracy, must be address by application of corporate resources. Sometimes it requires significant resource investment, both in personnel and finances. If the application includes public image damage control, the investment will likely be accompanied by loss of revenue. In the Sony Play Station hacking, the total investment and revenue loss amounted to almost $200 million, with an ongoing public relations challenge. It would have been far easier, and cheaper, to invest in pre-crisis planning model improvements.

7. Limitations

There are a few limitations to this case study. To start with, the present study employs a case study methodological approach. Generalization for a case study is challenging and should be approached with caution[23]. Future studies should be conducted to further analyze the detailed information in order to apply a general conclusion to a mass population. Nonetheless, the analysis of the Sony PlayStation hacking crisis provides valuable lessons to other companies that are at risk of hacking or theft of user information on what to do and what not to do when managing this kind of crisis.

Second, it is possible that a comparison of similar crises would yield more influential results. Perhaps, by contrasting how Sony has handled a crisis in the past and the PlayStation hacking crisis, a trend might emerge showing how Sony handles crises in general. Or juxtaposed, a compare/contrast method would yield information that proves Sony took severe missteps for the PlayStation hacking crisis only.

8. Conclusion

Sony made four primary mistakes when managing the 2011 hacking crisis. First, Sony failed to inform its customers about the breach until a week after the incident and Sony also failed to inform the customers that credit card information might have been stolen. Second, Sony did not act immediately to shut down the network. Third, Sony inaccurately accused a hacker group without the proper information. Finally, Sony gave a timeline for the network to be fully functional again, which it fails to meet. Through the application of each of these missteps to the AMCM, it is demonstrated how to prevent the same missteps from happening to another company. A proper pre-crisis communication management plan is integral to handling crises and thus, utilizing the AMCM is one way of accomplishing this goal. Implementation of the AMCM as a pre-crisis focused strategy can increase consumer and shareholder confidence, along with its flexibility in addressing human nature, and consequently may help save the company's reputation.

References

1. M. Hachman, Sony Playstation Network Hack nabbed personal info, maybe credit card information. PCMag.com (April 26, 2011). Http://www.pcmag.comarticle2/0,2817,2384353,00.asp.
2. S. Knafo, Sony playstation network hack is just the beginning of giant data thefts: Experts. *Huffington Post*, (2011, May 6). Retrieved from

http://www.huffingtonpost.com/2011/05/06/playstation-theft-sony-hack_n_858355.html
3. J. Tessler, Sony explains playstation network hack to congress. *Huffington Post*, (2011, May 4). Retrieved from http://www.huffingtonpost.com/2011/05/04/sony-playstation-congress_n_857811.html
4. M. Yamaguchi, Sony playstation network hack to cost $170 million. *Huffington Post*, M. (2011, May 23). Retrieved from http://www.huffingtonpost.com/2011/05/23/sony-playstation-network-hack-cost_n_865432.html
5. D. Goodin, User data stolen in sony playstation network hack attack. *The Register*, (2011, April 26). Retrieved from http://www.theregister.co.uk/2011/04/26/sony_playstation_network_security_breach/
6. M. Williams, Playstation network hack timeline. *PC World*. (2011, May 1). Retrieved from http://www.pcworld.com/article/226802/playstation_network_hack_timeline.html
7. L. Barton, *Crisis in organizations II*. (South-Western College Publishing, Ohio, 2001).
8. W. Coombs, *Ongoing crisis communication: Planning, managing, and responding*. (Thousand Oaks, CA: SAGE Publications, 1999).
9. K. Fern-Banks, *Crisis communications: A casebook approach* 2nd edn. (Mahwah, NJ: Lawrence Erlbaum, 2001).
10. C. Pearson, S. Misra, J. Clair and I. Mitroff, Managing the unthinkable. *Organizational dynamics*, 26(2), (1997) 51-64.
11. I. Mitroff, Crisis learning: The lessons of failure. *The Futurist*, 36(5), (2002), 19-21.
12. B. Olaniran, and D. Williams, Anticipatory model of crisis management: A vigilant response to technological crises. In *Handbook of Public Relations*, eds. R. L. Heath & G. Vasquez (Eds.) Thousand Oaks, CA: Sage, 2001), pp. 487-500.
13. B. Olaniran, and D. Williams, The need for anticipatory perspective in crisis communication. In *Pre crisis Planning, Communication and Management: Preparing for the inevitable* eds. B. Olaniran, D. Williams, and W. Coombs (Peter Lang, NY, 2012), pp. 13-17.
14. B. Olaniran, The role of perception in crisis management: A tale of two hurricanes. *Multicultural Education*, 15(2) (2007), 13-16.
15. B. Olaniran and D. Williams. (2004). Burkian counternature and the vigilant Response: An anticipatory model of crisis management and technology. In *Responding to Crisis: A rhetorical Approach to Crisis communication*, eds. D. Millar and R. Heath (Lawrence Erlbaum Publishers, 2004), pp. 75-94.
16. B. Olaniran, and D. Williams, Applying anticipatory and relational perspectives to the Nigerian delta region oil crisis. *Public Relations Review*, 34, (2008), 57-59.
17. J. Scholl, D. Williams, and B. Olaniran, Preparing for terrorism: A rationale for crisis communication Center. In *Community Preparedness and Response to Terrorism*, eds. H. O'Hair, R. Heath, and G. Ledlow, (Praeger Publishers, CT, 2005), pp. 243-268.
18. K. Weick, Enacted sensemaking in crisis situations. *Journal of Management Studies*, *25*, (1988), 305-317.
19. L. Smircich, and C. Stubbart, Strategic management in an enacted world. *Academy of Management Review*, 10, (1985), pp. 724-736.
20. R. Heath, and J. Sultan, Pre-Crisis management and communication: Slippery steps or solid footing? In. *Pre crisis Planning, Communication and Management: Preparing for the inevitable*, eds. B. Olaniran, D. Williams, and W. Coombs (Peter Lang, NY: 2012), pp. 101-123.
21. T. Jacques, Issue management as strategic aspect of crisis prevention. In *Pre-crisis planning communication and management: Preparing for the inevitable*, eds. Olaniran, B., Williams, D. and Coombs, W. (Peter Lang, NY, 2012), pp. 17-36.
22. J. Creswell, *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches (3rd ed.). (*Sage Publications, CA, 2009).
23. J. Maxwell, *Qualitative research design: An interactive approach*. (*3rd ed*). (Thousand Oaks, CA: 2013).
24. R. Yin, *Qualitative research from start to finish*. (The Guilford, NY: 2011).
25. P. Seybold, Update on PlayStation network and Qriocity. *PlayStation. Blog*, (2011, April 26). Retrieved from: http://blog.us.playstation.com/2011/04/26/update-on-playstation-network-and-qriocity/
26. B. A. Olaniran and J. C. Scholl. New England Compounding Center (NECC) Meningitis Outbreak: A Compounding Public Health Crisis. *International Journal of Risk Assessment and Crisis Management, 4*(2) (2014), 34-42.
27. B. Olaniran, J. Scholl, D. Williams, and L. Boyer, Johnson and Johnson phantom recall: A fall from grace or a re-visit of the ghost of the past. *Public Relations Review*, 38, (2012), pp. 153-155.
28. A. Martin, LulzSec's Sony hack really was as simple as it claimed. *The Atlantic Wire*. (2011, Sep. 22). Retrieved from: http://www.theatlanticwire.com/technology/2011/09/lulzsecs-sony-hack-really-was-simple-it-claimed/42851/
29. C. Williams, PlayStation hack: Sony blames Anonymous hacktivists. *The Telegraph*. (2011, May 5). Retrieved from: http://www.telegraph.co.uk/technology/sony/8494177/PlayStation-hack-Sony-blames-Anonymous-hacktivists.html
30. A. Martin, Sony blames Anonymous for PlayStation hack. *The Atlantic Wire* (2011, May 4). Retrieved from: http://www.theatlanticwire.com/business/2011/05/sony-says-it-found-anonymous-calling-card/37350/
31. Centers for Disease Control and Prevention Psychology of a crisis, *Crisis and Emergency Risk Communication*, (2002, September). Retrieved from http://emergency.cdc.gov/cerc/pdf/CERC-SEPT02.pdf
32. Entertainment Software Association Essential facts about the computer and video game industry. *Entertainment Software Association*, (2012). Retrieved from http://www.theesa.com/facts/pdfs/ESA_EF_2012.pdf

33. What's New (Ongoing), *Snopes*, from http://wwww.snopes.com/info/whatsnew.asp
34. Playstation 3 Community Forums (ongoing), Sony Corporation, Retrieved from http://community.us.playstation.com/t5/PlayStation-3/bd-p/22012