AN EXPLORATORY CASE STUDY OF REPUTATION MANAGEMENT

David Lynn Hoffman, Metropolitan State University of Denver, Management Department
Campus Box 78, P.O. Box 173362, Denver, CO 80217-3362, 303-556-3061
dhoffm20@msudenver.edu

Debora J. Gilliard, Metropolitan State University of Denver, Management Department
Campus Box 78, P.O. Box 173362, Denver, CO 80217-3362, 303-556-4682
gilliard@msudenver.edu

ABSTRACT

Social media enables organizations to create online presences but unfortunately also allows critics to attack covering a larger audience than historically possible. Many organizations believe in the benefits of a good corporate reputation but are overwhelmed by the new landscape enabling anyone armed with a computer to significantly damage their credibility. The paper uses the exploratory case approach to study how several companies have succeeded or failed in their online responses to crises. The exploratory case study approach can lead to new theories, paradigms, or strategic processes to cope with the new rules of social media engagement. This research found that GM was slow in reacting to the faulty ignition switch, Target was similarly lethargic in notifying its customers, and BP's initial responses were inadequate and inaccurate. Conversely, the Census Bureau responses nullified an attack by a US Senator and Primark's unique use of prepared customer responses negated its opponent's attacks. Other organizations should emulate the Census Bureau's and Primark's successes with prepared contingency plans, engaged customers to help in their defense, and prepared counterattack measures. This can only be accomplished by elevating reputation management to the strategic planning level with prepared contingency plans.

THE CASE STUDIES OF REPUTATION MANAGEMENT

The negative effects of GM's faulty ignition switch destroyed GM's reputation, cost at least $1.3 billion in one quarter, forced a recall of 30 million cars, caused at least 43 deaths, incurred a $35 million dollar fine, prompted Congressional investigations, and led to its CEO, Mary Barra, apologizing for the incident after finding a "pattern of incompetence and neglect." Its previous bankruptcy may not save GM because unearthed evidence shows that GM knew about the faulty switch for a decade and should have divulged the issue during the bankruptcy so the "new GM" may still be held accountable. The damage is ongoing as GM discovers that is internal processes were not followed allowing faulty switches to be installed in recalled vehicles to replace a faulty switch.

Target's security breach in December of 2013 released personal information of 40 million US and Canadian customers, brought down Target's stock, forced Target to spend an initial $100 million on a new encrypted card system, and resulted in a $61 million cost. Although Target acknowledged the leak in December of 2013, it was slow processing customer calls leading to a social media blistering.

The British Petroleum (BP) Deep Horizon incident spilled 200 million gallons of oil, cost $42.2 billion in initial cleanup costs, affected 25,000 jobs in surrounding communities, and cost numerous businesses their livelihood. BP was reluctant to acknowledge that it was their fault, published contradictory messages, and was slow fixing the leak.

Conversely, the Census Bureau, when attacked by Senator McCain for using expensive Super Bowl advertisements, countered quickly with accurate information verifying that the advertisements reached a wide audience, encouraged more participation, cost less than alternative methods, and resulted in an accurate census that was on time and on budget.

Similarly, Primark (a low cost retailer similar to Wal Mart in the US) was attacked by the BBC and other critics for low cost products, overseas sweat shops, and its ruinous effect on small competitors. Primark was prepared, replied via social media, used customers who defended Primark, and counter attacked the BBC who left the encounter with its reputation damaged from a fabricated BBC story.

CONCLUSIONS AND RECOMMENDATIONS

The ability of social media to attack an organization requires swift and accurate responses tailored to the crisis. First reputation management should not be relegated to a lower level unit but should be a priority of strategic planning at the executive level. Reputation maintenance should be a goal set by top level decision makers who are immediately available to create an image of an actively engaged and caring CEO. Implementation of this goal should include sufficient resources to have prepared contingency plans for various crises. Third, the best contingency plans include prepared customer comments or customers who are ready to defend the organization through their own social media. Finally the responses should be timely, transparent, and keep the public continually informed on how the organization is responding to the crisis.

REFERENCES AVAILABE UPON REQUEST