

Kelli, Kunath

Mark Glantz

Image Repair Assessment Project

FaceBreach: A Study on the Facebook Defensive Strategies and the Photo API Bug

INTRODUCTION

2018 has been an especially challenging year for Facebook® and founder, Mark Zuckerberg as related to security breaches. The company was currently under investigation by the FTC for privacy violations, “. . . the FTC takes very seriously recent press reports raising substantial concerns about the privacy practices of Facebook®,... confirming that it has an open non-public investigation into these practices.” (FTC, 2018, p. 1), after it self-reported significant security breaches with the discovery of being hacked September 13-25, 2018, when it later reported an additional breach. The additional breach though not as serious and which most likely also took advantage of security weaknesses that were in existence during the same period as the prior breach was announced in December of 2018. This paper will focus specifically on what these breaches involve, and for purposes of constraints in length on this paper, how the corporation handled the crisis using Benoit's Image Repair Discourse Theory on the lesser offense affecting 6.8 million users and identifying and then evaluating the strategies used.

On September 28th, 2018 Facebook® announced that a security flaw had been discovered which could have allowed up to 50 million user accounts to be compromised. The breach was the largest in the company's 14-year history according to the New York Times and other sources. This was later adjusted down to 30,000 by some reports and upwards of 87 million by another (Nieva & Wong, 2018, p. 3). On September 14, there was an unusual Facebook® account activity which alerted Facebook® that it was under cyber attack. “The vulnerability stemmed from Facebook®'s view as” feature, which lets people

see what their profiles look like to other people. Attackers exploited code associated with the feature and were able to steal “access tokens” they could use to take over people’s accounts” (Nieva & Wong, 2018, p. 3). The ability to steal a token is actually worse than stealing passwords because you don't even need a password to enter accounts if you have a token. The hackers were obviously very sophisticated in programming being able to discover a combination of 3 separate bugs that allowed for this crime to take place. Facebook® is currently working with the FBI and other country regulators to address this breach.

On December 14, 2018, Facebook® announced another security breach had taken place. This breach affected approximately 6.8 million users and specifically related to authorized and unauthorized access to account holder’s photos. “For a 12-day period in September, up to 6.8 million users’ private photos may have been revealed to 1,500 apps built by 876 developers” (Schwartz, 2018, p. 1). The breach in this crisis allows any of the approved apps to go beyond what the account holder already authorized to them view. It gives developers access to photos shared on their Facebook® stories and even to photos they had uploaded on their Facebook® accounts but had not uploaded yet or chosen to upload. To address this crisis, the corporation utilizes Benoit’s defeasibility, minimization, corrective action, and mortification/apology response strategies. As we will examine next, the mortification/apology response was ineffective, the minimization was effective and was especially helped in light that the previous crisis alone was so offensive and it is too soon to see if the other strategies have been effective.

REVIEW OF LITERATURE

Image repair specialist William L. Benoit emphasizes there is no perfect defense strategy for every crisis that occurs because each crisis is unique. That being said, there are categories of strategies that are best suited for each of these unique situations. In the following paragraphs, I will review some approaches used in this case study. We will describe his strategies below and then relate them to other published case studies in this genre.

Benoit states that repair strategies are organized into 5 categories: Denial, Evasion of Responsibility, Reducing Offensiveness, Correction Action and Mortification. (Benoit, 2015, p. 22). Denial is the most straightforward. There is simple denial (I did not do it), and shifting the blame. “Strategies for Evasion of Responsibility attempt to evade or reduce responsibility for the undesirable act. In such cases, one may not be able to completely deny responsibility but may attempt to reduce perceived responsibility for the act by adding new beliefs. One may claim to have been provoked and thus not solely responsible. A person may offer a defense of defeasibility, stating that the action was due to lack of information or ability, and hence not entirely one’s own fault.” (Benoit, 2015, p. 27). The Strategies for Reducing Offensiveness include: “Bolstering attempts to improve the accused’s reputation in hopes of offsetting or making up for the damage to the image from the undesirable act (this strategy uses beliefs and values about good things the accused has done). Minimization reduces the magnitude of the negative feelings attributed to the act, in hopes of lessening the ill feelings directed to the accused. It works by changing beliefs about the magnitude of the offensive act.” (Benoit, 2015, p. 29). Corrective Action. “In this strategy for image repair, the accused vows to fix the problem. This approach can take the form of restoring the situation to the state of affairs before the objectionable act and/or a promise to “mend one’s ways” and make changes to prevent the recurrence of the undesirable act. If the problem is one that could recur, the actor’s position may be enhanced by the provision of assurances that changes will prevent it from happening again”. (Benoit, 2015, p. 25). Mortification. “As

Burke (1970, 1973) recognizes, the accused may admit the wrongful act and ask for forgiveness, engaging in mortification. If we believe the apology is sincere, we may choose to pardon the wrongful act. Schonbach (1980) also discusses concessions, in which one may admit guilt and express regret. It may be wise to couple this strategy with plans to correct (or prevent recurrence of) the problem, but these strategies can occur independently. “ (Benoit, 2015, p. 26).

The following cases have been chosen with similar image repair problems to Facebook® :

Argument Strategies: Antidote to Tylenol’s Poisoned Image, Authors: William L. Benoit and James J. Lindsey; Dow Corning’s Image Repair Strategies in the Breast Implant Crisis, Authors Susan L Brison and William L. Benoit; and, A Critical Analysis of U.S AIR’s Image Repair Discourse, by William Benoit and Anne Czerwinski.

The Tylenol case was chosen as a comparison mainly because like Facebook®, was a victim of an unknown 3rd party attacker. Tylenol, however, utilized a very successful image repair case according to Benoit, and it would be very hard for anyone to disagree with that considering that at the time of the poisoning many thought the company’s image was so fatally damaged that it would never recover. Instead, with use of denial, and shift to bolstering strategies, Johnson and Johnsons’ Tylenol product fully recovered to its leadership position.

The Dow Corning case involved three phases to try to correct it’s image. But in the end they failed to repair their image and even ended up taking their product (silicone breast implants) off the market. In the first phase (July-September 1991), Corning used simple denial putting out a statement on July 18, 1991 stating that, ”implants do not increase the risk of breast cancer” (Brinson & Benoit, 1996, p. 31). During the second phase Corning used another strategy of image repair by using minimization to try to lessen the negative impact of the public by saying that documents "paint an inaccurate and incomplete picture" of the research done on the safety of silicone breast implants (Brinson & Benoit, 1996, p. 36). The attempts at image repair failed in this case. In the third phase they

finally used corrective action, however at this time it was too late to fully repair the company's image. (Brinson & Benoit, 1996, p. 36).

The U.S Air case was chosen as a comparison because like Facebook®, this corporation has been plagued with more than one recurring crisis situation resulting with what could be considered neglect by not following protective measures to protect their clients from harm. In this case, however, lives were lost which could be attributed to shortcuts taken by the company in mechanical safety measures. U.S. Air's strategies of using only pilots and upper level personnel to defend its image did not work well. It would have been more convincing if there was representation by some of their airline mechanics. In addition, the authors of this article state that denial and corrective action responses were not effective.

ANALYSIS

Regarding Facebook® 's security breach involving possible unauthorized use of account holder photos and announced on December 14, 2018, the corporation predominantly used Benoit 's and bolstering technique to reduce offensiveness.

Facebook® tells Josh Constine from Techcrunch “the bug did not impact photos privately shared through Messenger. The bug wouldn’t have exposed photos users never uploaded to Facebook from their camera roll or computer. But photos users uploaded but either decided not to post, that got interrupted by connectivity issues, or that they otherwise never finished sharing could have winded up with app developers.” (Constine, 2018, p.3). The company here is emphasizing the security of the client's photo privacy on their Messenger application and that of any photos the client had on their computer which were never uploaded to Facebook®, which can be considered a bolstering technique. “Facebook said ... it found and fixed the bug on Sept. 22, and it notified regulators in late November after an internal investigation to determine the scope of the incident.” (Romm, 2018, p.2). Acknowledgment of the photo security breach has come mainly over blog announcements and through

interviews with smaller tech journals. Perhaps this was purposeful to further reinforce the minimization strategy, but could also be a delay tactic to not expose too many breaches at once since it was originally discovered and corrected months prior along with the largest breach in the company's history. The company issued an apology to the account users that were affected through an email and used corrective strategies of fixing the breach. The first corrective strategy was to fix the software glitch. The next corrective strategy was achieved through contacting the 3rd parties who would have had access to the photos instructing them to delete unintended photos and also gave account holders instructions, in case they were still concerned about their photos, to go through their privacy settings to make sure they were comfortable with the amount of access they were giving the company. Finally, Facebook®, provided the affected account holder the list of apps that may have had access to their images during the process.

EVALUATION

Overall, this was really a damage control issue after coming off such a huge security break announced just a few months earlier. Using minimization and corrective action as corrective strategies response was successful in that it worked fairly well to not cause further damage to the corporation's badly tarnished name. However, to say this strategy worked to help repair their image would be going too far. Generally, Facebook® effectively handled their damage control with photo breach. Had the photo breach been announced along with the larger profile information leak and access token “give away”, Facebook® would most likely have had more criticism from their customer audience because they may have connected the dots more about how this could seriously affect them. By delaying the announcement and minimizing, the only real criticism they received is why wait so long for the official announcement.

CONCLUSION

Surprisingly, Facebook® still has a huge following with their audience despite the fact that their users' and subscribers' personal information was leaked out to millions. Perhaps they do not fully understand the damage this can cause them personally. The Government bodies on the other hand may not be as forgiving. The fines are heavy and litigation could be forthcoming. For instance, relating to the larger data breach crisis, "The social network could be fined a maximum of \$1.63 billion if it is found to have breached the General Data Protection Regulation (GDPR) in the European Union" (Kharpal, 2018, p. 1).

Other financial losses include those to shareholders. Stock prices have seen huge drops. Zuckerberg alone's net worth dropped 20 billion dollars as a result (Abbruzzese & Boyce, 2018, p. 1). An area that Facebook® certainly could have improved was during the prodromal stage (Fink) meaning the pre-crisis stage. Being experts in technology Facebook® management could have been proactive in setting another layer of security evaluation with new product feature introductions to catch oversights related to security weaknesses.

Work cited

Abbruzzese, J., & Boyce, J. (2018, December 29). Facebook's year has been so bad you probably forgot about most of this. Retrieved January 10, 2019, from

<https://www.nbcnews.com/tech/tech-news/facebook-s-2018-timeline-scandals-hearings-security-bugs-n952796>

Benoit, W. L., & Czerwinski, A. (1997). A Critical Analysis Of USAir's Image Repair Discourse. *Business Communication Quarterly*, 60(3), 38–57. <https://doi.org/10.1177/108056999706000304>

Benoit, W. L. (1997). Image repair discourse and crisis communication. Retrieved January 10, 2019, from <http://www.ou.edu/deptcomm/dodjcc/groups/98A1/Benoit.htm>

Benoit, W. L. (2015). *Accounts, excuses, and apologies: Image Repair Theory And Research*. Albany: State University of New York Press.

Constine, J. (2018, December 14). Facebook bug exposed up to 6.8M users' unposted photos to apps. Retrieved from <https://techcrunch.com/2018/12/14/facebook-photo-bug/F>

Isaac, M., & Frenkel, S. (2018, September 28). Facebook Security Breach Exposes Accounts of 50 Million Users. Retrieved from <https://www.nytimes.com/2018/09/28/technology/facebook-hack-data-breach.html>

Kharpal, A. (2018, October 03). Facebook could face up to \$1.6 billion in fines over data breach as regulators eye formal probe. Retrieved January 10, 2019, from <https://www.cnbc.com/2018/10/02/facebook-data-breach-social-network-could-face-eu-fine.html>

Lapowsky, L. M. (2018, September 29). Everything We Know About Facebook's Massive Security Breach. Retrieved from <https://www.wired.com/story/facebook-security-breach-50-million-accounts/>

Maring, J. (2018, October 12). Facebook October 2018 security breach: Everything you need to know. Retrieved from <https://www.androidcentral.com/facebook-october-2018-security-breach>

Romm, T. (2018, December 14). Facebook says a new bug allowed apps to access private photos of up to 6.8 million users. Retrieved January 10, 2019, from https://www.washingtonpost.com/technology/2018/12/14/facebook-says-new-bug-allowed-apps-access-private-photos-up-million-users/?utm_term=.e4e7d91c55cc

Schwartz, M. J. (2018, December 17). Ireland's Privacy Watchdog Probes Facebook Data Breaches. Retrieved January 10, 2019, from <https://www.bankinfosecurity.com/irelands-privacy-watchdog-probes-facebook-data-breaches-a-11865>

Statement by the Acting Director of FTC's Bureau of Consumer Protection Regarding Reported Concerns about Facebook Privacy Practices. (2018, March 26). Retrieved from

<https://www.ftc.gov/news-events/press-releases/2018/03/statement-acting-director-ftcs-bureau-consumer-protection>

Susan L. Brinson & William L. Benoit (1996) Dow corning's image repair strategies in the breast implant crisis, *Communication Quarterly*, 44:1, 29-41, DOI: [10.1080/01463379609369998](https://doi.org/10.1080/01463379609369998)

Turner, J. (2018, December 19). New Facebook Data Breach Exposes User Photos. Retrieved from <https://tech.co/news/facebook-data-breach-exposes-user-photos-2018-12>

William L. Benoit & James J. Lindsey (1987) Argument Strategies: Antidote to Tylenol's Poisoned Image, *The Journal of the American Forensic Association*, 23:3, 136-146, DOI: [10.1080/00028533.1987.11951338](https://doi.org/10.1080/00028533.1987.11951338)

Wong, Q. (2018, December 19). Facebook's terrible year just got worse: What you need to know. Retrieved from

<https://www.cnet.com/news/facebooks-terrible-year-just-got-worse-what-you-need-to-know/>