TWIT HAPPENS: HOW TO DEAL WITH TWEET REGRET IN THE PUBLIC SECTOR

Addressing social media mistakes, and recovering appropriately in order to protect your public entity and preserve your audience

ArchiveSocial
Social media archiving for government

CONTENTS

INTRODUCTION

Mistakes happen on social media, and there are good and bad ways to address them. This white paper highlights real-world examples and examines the types of issues government entities will inevitably encounter in their use of social media. Like social media itself, social media mistakes happen in real time, making it unlikely that the offending content can be removed before users share and possibly record it. However, that does not mean that it is impossible to recover from a mistake on social media. There are positive ways to approach these situations and ensure that the benefits of social media continue to outweigh its potential pitfalls.

TWIT HAPPENS #1: HASHTAG GONE WILD

What might go wrong

It is important for government agencies to experiment with social media, but unfortunately, an experiment or marketing campaign can sometimes backfire. A prominent example comes from a recent Twitter campaign conducted by the NYPD Police Department. Attempting to follow in the success of Twitter brand campaigns such as #McDStories and #ILoveWalgreens, the official account of the NYPD encouraged Twitter users to tweet the hashtag #myNYPD and include a picture of themselves with a police officer. The campaign quickly backfired, and Twitter users began to share photos of alleged police brutality instead.

The consequences

NYPD's simple hashtag idea turned into a public relations disaster. #MyNYPDbecame a trending topic on Twitter, and the antipolice sentiment spread to other geographies such as New York and Los Angeles. The mainstream media soon picked up on the story and continued to add fuel to the fire. Not only did the negative reaction on social media serve as an embarrassment to a well-intentioned campaign, but it was also a disheartening experience for the countless police officers who have dedicated their lives to making a positive impact in their communities.

How to recover

NYPD received significant criticism for the #MyNYPD campaign, but it is instructive to understand the way in which they responded. Specifically, New York Police Commissioner Bill Bratton made it clear that he "welcome[d] the attention", because it allowed them receive feedback from the public and have an open conversation the about perception of the police department. He also pointed out that the negative photos were largely "old news." As demonstrated, perhaps the best way to deal with an unexpected reaction to a marketing campaign is to first accept the reaction. You can then decide if it makes sense to suspend the campaign, and perhaps even embrace the conversation to potentially steer it in a more positive direction. Commissioner Bratton was able to turn the hashtag disaster into a learning experience for the department, as well as distance the current police department from transgressions in the past. This is a wise approach, because rather than try to ignore negative fallout, you can acknowledge it publicly and use the opportunity to emphasize the continuous improvement of your organization.

TWIT HAPPENS #2: THE HASTY COMMUNICATION

What might go wrong

A hasty communication to citizens can cause unrest, misinform those in need, and hurt relationships with partners and the public. During the SXSW 2014 convention in Austin, Texas, the @austintexasgov Twitter account decided to tweet out a phone number suggesting that the public bring forward potential complaints about their very own police department.

The consequences

Naturally, police officers who had been working long hours to protect the public, and who were in no way creating problems, took offense and were "completely demoralized". Even though the City of Austin did not intend to undermine its own police operation, the hasty wording of the tweet was seen as divisive and led to significant media coverage.

How to recover

To their credit, the City of Austin quickly issued a statement apologizing for the tone of the message and utilized the @austintexasgov account to tweet a public apology to the @Austin_Police Twitter account. In situations involving a misunderstanding, it is critical that there is both a genuine apology and an emphatic clarification regarding the intent of the original communication. Austin responded in exactly such a manner. Apologizing via Twitter was also a smart move because it helped address the misunderstanding exactly where it originated.
In general, it is important to ask yourself questions like "Who am I affecting with this tweet?" and "What are the possible outcomes?" before impulsively hitting the tweet button. In addition to thinking about your audience, you must remember your own organization and colleagues. Damaging your own reputation, or your working relationships, is far worse than getting information out a few minutes later. If you take a moment to consider the worst-case interpretation of your words, then in reality, you will almost always avoid it.

TWIT HAPPENS #3: FAILING TO COMMUNICATE TO CITIZENS

What might go wrong

On the exact opposite end of the spectrum, failing to communicate to citizens can be just as bad as communicating in haste. During the swine flu outbreak in 2009,panic spread across Twitter with false rumors regarding germ warfare and contaminated meat. Government health organizations at both the national and international levels were noticeably absent from the social media conversation, allowing the misinformation to reach alarming levels.

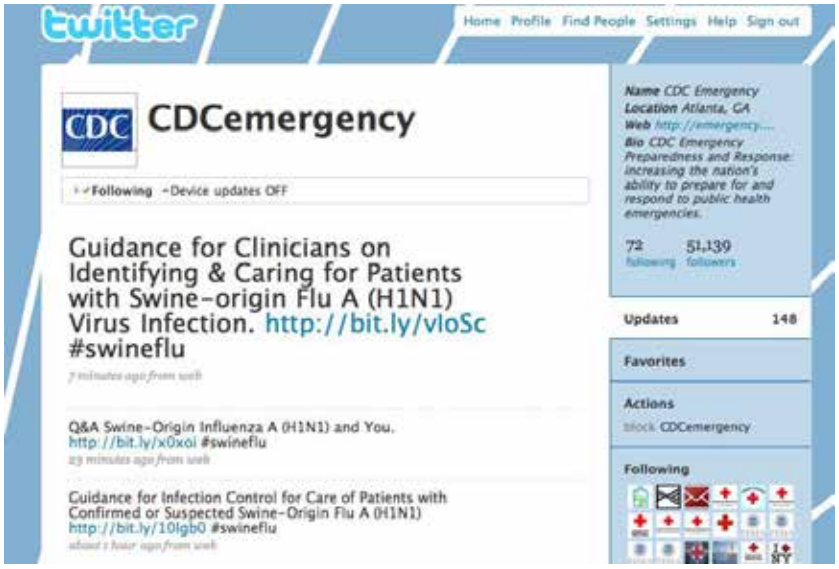
The consequences

This situation highlighted the potential dangers of social media, and to some extent, led to increased caution and concern from agencies already nervous about social media. Organizations such as the Center for Disease Control and Prevention (CDC) and World Health Organization (WHO) were criticized for not doing enough to combat the spread of misinformation. Most significantly, the rumors spreading across social media created unnecessary panic within the general public.

How to recover

Unfortunately, by the time a failure to communicate becomes obvious, it might be too late to recover. Regardless, the situation can be evaluated to best understand how to avoid communication gaps in the future.

During the swine flu outbreak, health organization should have been at the forefront of the social media conversation. Statements should have been released promptly at the start of the epidemic, and continually updated with the latest



developments. To their credit, the CDC was issuing official status updates and action plans regarding the disease. However, the CDC and others could have done much more to actively participate in the conversation by replying to tweets anddiscrediting false information.

Furthermore, when dealing with a high profile situation that can shake public confidence in your organization, it is worthwhile to perform a retrospective and create an action plan for the future. In fact, using social media to share your action plan is a good way to reinforce your commitment to communicating more effectively.

TWIT HAPPENS #4: GETTING HACKED

What might go wrong

Hacking can damage a company's image as a reliable source and can substantially affect public action and opinion. It is also one of the most difficult social media mistakes to prevent.
In April of 2013, hackers took over the Associated Press account on Twitter and falsely claimed that explosions had occurred at the White House. The Associated Press is widely considered one of the most reliable sources of news, and the tweet was taken very seriously. Even though the tweet was only available for a few minutes, it received over 3000 retweets before Twitter took the account offline.

The consequences

Although the Associated Press was the target in this situation, the US economy was the true victim. The Dow Jones industrial average plunged 143 points immediately following the hacker's tweet, creating an estimated $136.5 billion dollar loss in value within a matter of minutes. Fortunately, the tweet was quickly discredited and the stock market recovered soon after.

How to recover

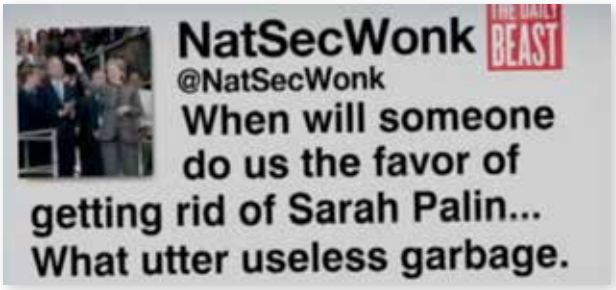
Getting hacked stinks, so how you react is what matters. The best course of action is to remove the content as quickly as possible, and do everything you possibly can to notify your audience of the situation. Within minutes, the Associated Press leveraged its other Twitter accounts to discredit the false tweet and report the hacking. Other media outlets picked up on the correction and the stock market was able to return to normal levels.

In addition to acting fast, steps should be taken to prevent future hack attacks. An organization can lose credibility – within social media and beyond – if it is hacked on multiple occasions. Social media password credentials must be protected in the same manner as credentials for other important systems. And finally, employees should be trained to recognize and report hacking attempts such as spoofing and phishing attacks.

TWIT HAPPENS #5: EMPLOYEE GONE ROGUE

What might go wrong

Employees will make mistakes. Sometimes they are honest mistakes, and sometimes they are intentional. For example, in 2011, a White House national security official by the name of Jofi Joseph created an anonymous Twitter account criticizing government policies and employees, including President Obama. The Twitter account, @NatSecWonk, became known for ridiculing the Obama administration and criticizing many of Joseph's own colleagues.



The consequences

After months of investigation, Joseph was identified as the author of the Twitter feed and was fired from his position in the White House. However, the damage had already been done. The @NatSecWonk Twitter account had become well known within the Washington DC Beltway and was a source of frustration for many public officials. Joseph was a senior official within the national security staff, and to some extent, betrayed the trust of his colleagues. Fortunately, there is no evidence that he leaked sensitive national security information.

How to recover

When dealing with a rogue employee, it is critical for the organization to immediately distance itself from the employee and act decisively. Otherwise, the organization bears the risk of accepting responsibility for the employee's actions.

The White House acted appropriately in this situation by firing Joseph and letting him take full responsibility for his actions. Joseph shutdown the Twitter account and also issued an apology stating, "It has been a privilege to serve in this Administration and I deeply regret violating the trust and confidence placed in me." In other words, once unmasked, he understood the true consequences of what he had done.

Every organization has its own polices and rules of conduct. It is important to train employees and make them aware of what constitutes acceptable behavior. Therefore, if an employee decides to deviate from the accepted rules of conduct, all parties will understand what needs to happen.

CONCLUSIONS

• It is essential to experiment and innovate with social media, but remember that your audience will ultimately dictate the end results. Be prepared to embrace the unexpected.

• Always consider the potential outcomes and interpretations of what you say, and be transparent about your intentions when you are misunderstood.

• Remember that participating in the conversation is the only way you can help steer the flow of information. As a public entity, you might actually bear responsibility for ensuring that the public remains accurately informed.

• Hacking is an unfortunately reality in the digital world. Do whatever you can to contain the damage, and always take the security of your social media credentials seriously.

• Empower your employees but never sacrifice the behavioral standards of your organization. Ensure that rules of conduct are well understood, and be ready to enforce them.

• Recognize that mistakes will happen, and remember that how you handle those mistakes is really what matters in the end.

ABOUT THE AUTHOR

Anil Chawla is an experienced technologist and entrepreneur, with a proven track record of working with businesses to address challenges related to social media. He has over a decade of experience creating software products, and has spent the last 4 years developing social media technology. Mr. Chawla and his work have been featured in prominent publications including *Government Technology, NextGov, InformationWeek, Fast Company,* and Entrepeneur.com. Mr. Chawla received a B.S. degree in Computer Science from Georgia Tech, where he graduated at the top of his class. Mr. Chawla is the CEO of ArchiveSocial, which he founded to help government organizations navigate the important legal and regulatory challenges they face related to social media management.

Additional papers, articles, and free trial offer available at http://archivesocial.com

About ArchiveSocial

ArchiveSocial enables public entities to safely and effectively utilize social networks such as Facebook, Twitter, YouTube, and LinkedIn. ArchiveSocial is the industry's first archiving technology providing 100% authentic capture of social media for compliance with state and federal records laws such as FOIA. It provides a legal safety net, and eliminates the time and effort required to respond to public records requests. ArchiveSocial is completely hosted and requires zero IT deployment. It serves as a cost effective offering for any sized public entity, and provides the industry's easiest and most comprehensive solution for managing records of social media. ArchiveSocial is based in Durham, North Carolina.

ArchiveSocial

Social media archiving for government

Additional papers, articles, and free trial offer available at **archivesocial.com**