BUILDERS UNDER FIRE

RESPONDING TO SOCIAL MEDIA ATTACKS

by Stephen Yoch, Felhaber Larson

Businesses increasingly rely on the internet and social media to attract and retain customers. Responding to online attacks is critical to maintain a strong online reputation. Even one incident can ruin a company's reputation and cause customers to go elsewhere.

Gone are the days when complaints were spread through word of mouth. Attacking a company online is easier and more effective. Anyone can post a bad Yelp review or damaging Twitter post. More sophisticated attackers can impersonate a company online, hack accounts, and reach millions of users often before a company ever notices.

PROACTIVE MEASURES

Harm posed by an attack is greater if the victim company has no detection or response plans in place. There are steps a company can take to limit the harm caused by an attack.

- **MANAGE AND MONITOR.** A company should invest in continuously monitoring its online presence.
- **COMPLAINT PROCEDURE.** A company should create clear procedures with a designated team to investigate and respond to posts containing damaging rumors or misleading information. The faster a company responds to complaints, the more likely any single attack will be contained.

COMBATTING AN ATTACK

STEP 1 **DO NOT ACT IMPULSIVELY OR RETALIATE.** The initial reaction to a social media attack is to strike back. A vengeful response, without fully understanding the attack, can do more harm than good. Instead, take a deep breath, consider options, and make a proper response.

STEP 2 **IDENTIFY THE NATURE, SOURCE, AND EXTENT OF THE ATTACK.** It is crucial (but not always easy) to identify the attackers. Anonymous posting is very common. If the attacker(s) cannot be identified, a company should at least identify the type of attacker, who may be an angry or dissatisfied:

- Customer
- Competitor
- Employee
- Investor
- Extortionist
- Consumer watchdog

To determine its response, a company should search online to identify all social media platforms (e.g. YouTube, Facebook, Twitter, Snapchat, Yelp, Google Reviews, etc.) on which the attack is taking place or being discussed.

STEP 3 **EVALUATE POTENTIAL RESPONSES.**

A. **Contact Media Platform.** Contact the platform provider directly or utilize the provider's reporting mechanisms. For example, Yelp allows reporting and removal of fake or defamatory reviews, and Twitter and Facebook allow reporting and blocking of harmful or abusive users. If the damage can be contained using these procedures, this should be the first option.

B. **Contact the Known Attacker Directly**. A disgruntled customer or employee may respond more positively if contacted personally. Research has found that approximately 1/3 of customers receiving a personal response to their negative review deleted the negative review and/or posted a positive review.

C. **Reaching Out to Unknown Attacker.** By posting a polite message asking the attacker to contact the company directly, a company may cure the underlying problem that triggered the online attack, and will show other viewers that the company is attentive to its customers.

D. **Issue Public Statement.** The more individuals publicly expressing concern, the more appropriate a public statement becomes. To the greatest extent possible, a company should carefully draft its response to frame the issues positively. The message should focus on affirmative steps taken to remedy a legitimate concern raised by an attacker.

STEP 4 **LEGAL ACTION.** A final option is to pursue legal action, including hiring an attorney to send a cease and desist letter, or file a defamation claim. While defamation claims are notoriously difficult to prove, some organizations have been successful against blatant and unfair attackers.

CONCLUSION

Time and money are well spent monitoring social media and having a team in place to respond quickly to an attack. Rapid and effective action can mean the difference between a minor annoyance and a major PR disaster.

STEPHEN YOCH, FELHABER LARSON

Stephen Yoch is a partner at Felhaber Larson and has been representing builders and developers for over 20 years. Over the last decade, he has developed an expertise in cyber security, focusing on construction companies. He received a cyber security certificate from Mitchell Hamline Law School in 2016.
syoch@felhaber.com