Disinformation is harming businesses. Here are 6 ways to fight it

By Matthew F. Ferraro for CNN Business Perspectives
Updated 5:41 PM ET, Mon June 10, 2019

Editor's Note: *Matthew F. Ferraro is a former intelligence officer, a senior associate at WilmerHale, term member of the Council on Foreign Relations, and a visiting fellow at the National Security Institute at George Mason Law School. The opinions expressed in this commentary are his own.*

Last month, a video that appeared to show House Speaker Nancy Pelosi slurring her words went viral on social media. This video, which was edited and slowed for effect, was viewed millions of times, and political opponents used it to question Pelosi's health.

The video represents a rudimentary example of the next chapter of disinformation — realistic, artificial intelligence-enhanced forged videos known as "deep fakes" that can make it look like people are doing things they never did and saying things they never said.

Politicians have raised the alarm about the threat such fakes pose to politics. But what is less often discussed — yet just as dangerous — is the threat deep fakes and disinformation more generally poses to corporations, brands and markets. We have already begun to see the effects of the intentional and covert dissemination of false information on businesses, even without the added dangers of manipulated videos.

For example, in August 2017, a pediatric medical practice in Pittsburgh posted a video about the importance of the HPV vaccine only to find itself inundated by thousands of false negative user reviews. The origin? Anti-vaccination activists in 36 states and eight countries who coordinated the deluge.

The same month, tweets with the Starbucks company logo claimed the coffee chain was hosting a "Dreamer Day" and offering free drinks to undocumented

immigrants for a limited time. Starbucks was forced to respond on social media that the tweets were untrue.

In October 2018, after semiconductor giant Broadcom announced its intention to acquire CA Technologies for $19 billion, a memorandum made to look like it came from the US Department of Defense warned that the US government would review the transaction for potential national security threats. Broadcom's shares fell when the memo was exposed as a forgery.

This problem will only get worse as disinformation attacks become more common and as deep fakes become more convincing and their use more widespread in both political and business spheres. So what can corporations do to protect their brands and valuations from disinformation? Businesses and institutions should consider the following six measures that they can take before, during and after a fake-news attack.

Social listening

Successful companies understand their markets, their customers and their partners. They also need to understand how their brand is perceived on social media — either by using in-house technology or hiring an outside firm. By doing so, companies can get advance warning of an individual's or group's efforts to spread disinformation about a brand. Businesses should establish verified accounts on the major social media platforms and use them regularly to establish trust with their markets.

Self-assessment

Attacks may be timed to do maximum damage to a brand and provide maximum benefit to a malefactor. IPOs, mergers, acquisitions, major investments and product launches can all be inviting targets for disinformation. Consider the phony memo circulated about the Broadcom-CA Technologies acquisition; it was plainly timed for a moment when investors would be most attentive.

To prepare for such attacks, corporations should look in the mirror. What upcoming events carry the greatest risk? What aspects of the business are most vulnerable to attack? What messages would have the most resonance? Honest inventories are a critical form of preparedness, and the sooner corporations conduct them, the better.

Preparation

Corporations cannot simply hope to design an effective response strategy after bogus tweets start trending. They need to prepare for such events, similar to how they plan for cybersecurity breaches. They should assign different responsibilities to members of an incident response team, like the director of IT, the head of communications and the general counsel, among others, and they should run drills for disinformation attacks.

Platform engagement

If a corporation is conducting appropriate social listening, it should be able to spot a fake-news attack early on before it balloons out of control. Once it recognizes what is happening, the company should identify the accounts and users propagating the disinformation. To get the bad actors' accounts frozen or shuttered, the company should contact the social media platforms being used to spread offensive content and prepare evidence for each platform to show how the Terms of Service are being violated. Vendors and law firms can help with this.

Communications

Sometimes, the best response to bad speech is more speech. The same is true here. Corporations need to communicate directly with their customers, the media and the public at-large to debunk fakery. For example, after the "Dreamer Day" posts started circulating, Starbucks engaged directly with Twitter users who were reposting fake "ads." And the pediatric practice targeted by anti-vaxers is working to assemble a pro-vaccine "virtual cavalry," as the CEO says.

Litigation

Finally, corporations can go to court against fake-news purveyors. Free speech rights protect opinions, but businesses are not defenseless when their brands are defamed or markets manipulated.

Possible claims include those for defamation and trade libel; economic torts like those that bar dishonest interference in a business's future economic relationships, deceptive trade practices and unjust enrichment; and federal trademark infringement for fraudsters who incorporate a company's logo into their posts.

Companies will want to consider the facts of each situation and the benefits and drawbacks of litigation and discuss the situation with outside counsel before filing suit.

Taking these steps won't inoculate a business against viral digital falsehoods, but they can help build resiliency and reduce the damage that disinformation can do to a company's reputation and value.

URL: https://www.cnn.com/2019/06/10/perspectives/disinformation-business/index.html