DEFENDING AGAINST THE VIRTUAL SMEAR

A "cybersmear" is a special kind of virtual attack that risks tarnishing a company's brand

By Rod Christie-Miller and Jenny Afia, Schillings and Andy Rivett-Carnac, Brunswick, London

For a company, a "cybersmear" can unfold like the plot of a Franz Kafka novel. Unidentified perpetrators launch a public smear campaign that seems to grow organically and in such a way that it becomes increasingly difficult to combat. It is like a man being falsely accused – he knows he is innocent but the concocted evidence puts him in the position of having to *prove his innocence*. It can be as grave a development as a cyber security breach (see *Once More Unto the Breach*, page 59), but more insidious and requiring a different mode of defense; it is analogous to libel.

Consider the case of a fictitious energy company called, let us say, SparkCo, the details of which are not far removed from some real-life situations. SparkCo's overworked head of communications, Jo, checks her BlackBerry before breakfast one morning and sees, buried among the standard summaries and spam, a startling Google update that jolts her wide awake. The headline reads: "SparkCo CEO embezzled company funds."

Jo uneasily clicks on the link, taking her to a *Huffington Post*-style blog site she's never seen before. The article, based on spurious quotes from an "unnamed senior employee," also carries what it claims to be details of the CEO's personal tax records. Fuzzy facts are sprinkled in with false quotes, turning the piece into a compelling cocktail of half-truths, complete fabrication, and outrageous anti-SparkCo propaganda.

Jo heads to the office, hoping that the unfamiliar blog is too obscure to be noticed. At her desk, she Googles the company and is shocked to find that her general search now throws up a link to the same article on the initial page of results. So much for not many people seeing it.

As usual, SparkCo's second Google result is its Wikipedia entry and Jo is dismayed to see that this has been updated overnight, repeating the false allegations and containing a link to the original article as its sole source.

This bears all the hallmarks of a coordinated cybersmear campaign, probably one that was originated by a group with some sort of agenda rather than by a disgruntled employee. In any case, if this is not adeptly managed, it could compromise an invaluable asset for any company: its reputation.

As she begins to process the questions and concerns running through her mind, Jo is

interrupted by a colleague asking if she's seen the new post on the company's popular Facebook page which links to the article entitled "SparkCo CEO embezzled company funds" on the *Huffington Post*-style blog site. Jo pulls the page up to see five similar posts sitting atop the Facebook "wall."

Jo's phone rings. A well-known business journalist is on the phone requesting a comment about a tweet by SparkCo's CFO. Jo, who wasn't even aware the CFO was on Twitter, says she'll call him straight back. The journalist warns her that the newspaper is going to press within the hour with a "page lead" on SparkCo, so he needs a response quickly.

A prompt Twitter search turns up a tweet with the CFO apparently berating the CEO's management style. A follow-up reads: "Still, won't have to put up with it much longer #SparkCo." Jo's search also brings up a tweet linked to a think tank report: "Three energy companies in peril," including a section on SparkCo with negative comments from experts.

As Jo's morning coffee cools on her desk, she fears – with good cause – that these slurs are spreading like wildfire and rapidly solidifying into negative public perception of her company.

So what can be done when faced with the swelling tide of an anonymous cybersmear attack? The strategy should be to fight fire with fire. But first it is important to identify each and every outbreak of smear and document it carefully. The social media strategy and internal relationships between corporate communications, investor relations, marketing, and customer services should all be brought into play as the rebuttals begin. And in this world of ubiquitous social media, with instant, global access, those rebuttals need to begin as quickly as possible.

First in line for a response would be the prominent journalist, who would receive a courtesy call followed by a public @ message on Twitter directing him to a statement or press release on the SparkCo website that categorically denies the report as a smear. He should be urged to retweet and spread the message far and wide.

In tandem with the first step, a wider audience – employees, journalists, bloggers, regulators, business partners and investors – should be contacted and assured of the falsity of the claims and directed to the same press release.

It is then time to try and identify who was behind the attack. The SparkCo case almost certainly would be one of targeted malice, but sometimes an apparent cybersmear can turn out to be the result of simple computer error.

In 2008 a *Google News* software glitch resulted in a United Airlines bankruptcy filing from six years before, running as if it were breaking news. An analyst from *Income Securities Advisor*, an advisory firm, repeated the mistake in a newsletter which was, in turn, redistributed by *Bloomberg News*, the financial newswire, to hundreds of websites and other news outlets.

> "The strategy should be to fight fire with fire. But first it is important to identify each and every outbreak of smear and document it"

Compounding the mistake, Google's "newsbot" interpreted the story's popularity as confirmation of its importance, making the story even more prominent on the *Google News* website. By the time trading was halted, United Airlines' shares had fallen 76 per cent. The company was able to deny the rumor but its stock still closed down 10 per cent on the day.

In SparkCo's case, knowing what and who is behind the attack is crucial for planning a defense. When faced with anonymous attacks, using both technical and legal tools can be helpful in unmasking the perpetrator. In England, for example, a "Norwich Pharmacal Order" (NPO, named for a precedent case) compels an internet service provider (ISP) or webhost to disclose the identity and contact information of the person behind the offending online material. These can be obtained within a matter of hours if needs be.

In the US, New York state courts have ordered the disclosure of the identities of anonymous bloggers, when the applicant has demonstrated a good prospect of succeeding in a legal action against the blogger if he or she could be identified. The standard for obtaining an order varies from state to

state, though the basic rule is that if the applicant is able to show that a cause of action exists and is likely to be successful, the courts will consider assisting in identifying the proper defendant.

Often, being successful in uncovering online attackers requires a degree of perseverance in order to track down leads. The information obtained initially might not be trustworthy as savvy attackers take steps to cover their tracks. Yet even with the most sophisticated online smears, there will often be a trace somewhere that leaves a digital footprint or clue.

Once uncovered, the best legal strategy can be decided. Sometimes legal action will be appropriate. Laws of defamation apply just as much to online comments as they do to other forms of media. Faced with the ever-expanding technical means at the disposal of online defamers, the English courts have shown that they are willing to adapt old laws to modern situations. They have allowed the service of orders via Twitter and Facebook, for example, when it was the only way of ensuring the offenders would receive notice of the order. There are times when a legal response to the smearer may not be suitable – there is no one-size-fits-all solution for dealing with online smears. But one constant theme is that when attackers lose their cloak of anonymity, they quickly lose their power.

To run through the steps Jo could take to unmask the perpetrators of the SparkCo smear:

THE BLOG POST

SparkCo might not want to engage with the publisher of the blog site directly without knowing how it is likely to react (for example, will it revel in the attention and publicize the complaint?). Instead SparkCo might consider contacting the ISP/webhost to ask that the defamatory content be removed from the blog. Certainly, under English law if an ISP wants to use the "innocent dissemination" defense, it will want to do so promptly. Consequently, a complaint often yields fast results. However, there are limitations to this approach. If the site is hosted in the US, the ISP could point to Section 230 of the Communications Decency Act of 1996, which provides immunity for user-created content, no matter how false or offensive. Even if provided with absolute proof that content is false and seriously damaging, many ISPs will claim to have no duty to remove it.

THE GOOGLE ADWORD

A practical solution might be to reduce the visibility of the site. In SparkCo's scenario, Google would almost certainly remove the advert promoting the blog site from SparkCo's Google search results. The terms of Google AdWords – Google's main advertising product – prohibit advertisements that "include accusations or attacks relating to an individual's personal life." Applying to Google should see the link removed from SparkCo search results within a couple of hours.

THE CFO'S "TWEETS"

Jo is assured by the CFO that he has never tweeted in his life. It transpires that a fake account has been set up in his name, not just on Twitter but also on LinkedIn. Twitter and LinkedIn have procedures to disable false accounts after confirmation that the identities are bogus. Results can be achieved quickly.

THE THINK TANK "REPORT"

A little research reveals that the organization is highly dubious. Contact numbers listed on the site, for example, are not answered and the experts quoted in the report claim to have no knowledge of it. A court order to identify who posted the report online could be sought and obtained within a very short time. Assuming that the person identified is just a technical flunky being paid to carry out the attacks, SparkCo could consider seeking an order against that person compelling him to disclose the identity of his client, thus revealing whoever is masterminding the campaign.

SPARKCO'S WIKIPEDIA PAGE

Armed with the evidence to show that the damaging claims have emanated from discreditable sources, it will be possible to have the offending claims and links removed from SparkCo's Wikipedia page. Wikipedia has its own reputation as an authoritative source to protect. It is advisable to contact Wikipedia directly and request that the offending content be removed rather than try to change it oneself, as this can just lead to a frustrating cat and mouse game.

Wikipedia, by contrast, can permanently ban users from amending page entries. A constructive dialogue with Wikipedia's "Administrators" through the article's "talk page" will result in the material being removed if it can be shown to be disreputable and borne out of malevolent motives. If provided with sufficient evidence that the claims are unreliable, Wikipedia can remove material shortly after being contacted.

SPARKCO'S FACEBOOK PAGE

Finally, what about SparkCo's Facebook page, which has been tarnished by the negative posts? A cause of action can usually be found when a brand is hijacked in this way. For instance, there could be a potential defamation claim. However, more often than not in these situations, a legal approach would be counterproductive. The point about social media is that the brand is attempting to be sociable. There is no quicker way of alienating your newly sought friends than by suing them. Better to set up "house rules" on the page in advance, stating that defamatory or hateful posts will be removed. This gives a company's representative recourse to explain his motives when removing unsuitable content from its Facebook page.

CONCLUSION

There is much that can be done when confronted with an online smear. Brands that cope best are frequently those with a coordinated legal and PR strategy, alongside an organizational structure that allows for rapid responses to breaking issues. Companies that have a degree of goodwill from their stakeholders are much better placed to reach out to their wider audiences and call on them to help rebut false claims.

Yet, as cybersmears become more sophisticated, there is a broader cultural shift that is required to deter behavior that in other circumstances could be deemed criminal. The biggest change required is in attitudes toward online anonymity, particularly in the US. While the courts might be coming round to the idea that there should not be an automatic right to anonymity when posting content online, there is currently no requirement that websites, hosts, or ISPs collect or store any information that could be used to connect online activity to a real person, whether directly (such as storing a name) or indirectly (such as storing an IP address). Such technical and legal limitations create a profound lack of accountability on the web in the US.

In the UK, further legal redress may be on the way. A report ordered by Parliament calls for swift action by a host or ISP if the subject of anonymous material complains. It also calls for a cultural change, supported by legislation, that would mean anonymous online material should not be regarded as reliable.

A cultural shift will be hard to achieve. As demonstrated by the famous Stanley Milgram experiments in the 1960s, behavior becomes more extreme when people cannot see or identify with their victim. Participants in that experiment were willing to administer what they thought were brutal electric shocks (the "victims" were actors) when they could abdicate responsibility to someone giving orders.

Also, anonymity can be regarded as a force for good in the online world in some cases – allowing people to speak out against oppressive regimes, for example. But anonymity as the default position online clearly has its dangers and the harm that online smears can inflict must be recognized. Companies must embrace the digital age and governments need to provide sufficient protection. A first vital step toward achieving this would be to require that ISPs hold identifying information for those who post online anonymously, but that their identities be kept confidential unless there is proof that they have smeared another party.

Randi Zuckerberg, Facebook's former marketing director, declared earlier this year that, "Anonymity on the internet has to go away." Some other Facebook and Google executives concurred. After all, as a *New Yorker* cartoon caption once put it: "On the internet, nobody knows you're a dog."

Rod Christie-Miller is a lawyer and Chief Executive of **Schillings**, a London-based law firm that specializes in protecting and managing the reputations of international corporations, brands and high-profile businesspeople. He is an expert on defamation, privacy, and breach of confidence. **Jenny Afia** is a Senior Associate at the firm and focuses on reputation protection. *www.schillings.co.uk*

Andy Rivett-Carnac is a Director in Brunswick's London office, specializing in digital and social media.