National Cybersecurity Institute Journal
Volume 1, No.2

The New Demands of Online Reputation Management

Shannon M. Wilkinson, CEO Reputation Communications | Editing and Research by Christopher Hampton

ABSTRACT

The explosive growth of the Internet has dramatically changed the demands of reputation management. There are few barriers to publishing online, and every author has at least the potential of reaching broad audiences. There are also few laws regulating online information. Content is often posted anonymously, and website operators have legal immunity over what is posted on their sites. In many cases there is no one to prosecute, and no leverage to demand retractions.

Online reputation management first appeared in the mid-1990s, and has grown along with Internet use. These changes have also forced a much more proactive stance toward the protection of brand integrity. Security professionals now have a broad mandate for investigating, addressing and resolving online threats to the reputation of their company and its executives.

This paper gives an overview of the leading online reputational threats faced by companies in the United States, as well as an explanation how such events unfold, the motivations behind them, and how they can be protected against and resolved.

Threats discussed range from the dissemination of the home addresses and family information of executives to the leaking of internal company documents by inside sources, targeted online defamation campaigns, and the impersonation of executives on social media and other platforms, in addition to more conventional public relations crises.

The best tactics for avoiding many of those crises are proactive. They include online monitoring of the company brand and executives' online presence, as well as of social media sites maintained by family members. Company executives in particular should be made aware of online security practices, including protecting their data and using encryption for online correspondence. Most importantly, the company should establish a strong online presence, including interactive forums where company representatives can address grievances.

Effective planning will protect a company against many reputational threats. Reactive ORM techniques are increasingly focused on the production of quality content. The manipulation of search engine results—what used to be considered the central activity of ORM firms—has lost its utility as search engine algorithms have grown more sophisticated.

THE NEW DEMANDS OF ONLINE REPUTATION MANAGEMENT

The EU's recent passage of the "Right to Be Forgotten" law gives European citizens the ability to force Google and other search engines to remove links to embarrassing or irrelevant information.

The passage of that law increases the contrast between legislation regarding online publishing in Europe and the United States. In the U.S. there are still very few legal boundaries constraining the publication and distribution of online content. Authors are free to post most any material anonymously. If

anyone finds that material to be damaging, they have little leverage to demand a retraction and no clear target for prosecution. Discussion about new legislation has revolved around freedom of speech issues, issues that have advocates including such well-funded organizations as the Electronic Frontier Foundation.

In the U.S., the main law governing the Internet is Section 230 of The Communications Decency Act, which frees website owners from legal responsibility for what others post on their sites. It states, "No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider."

Understanding the implications of that law and how it impacts the privacy, security and reputations of U.S. citizens is recommended for cyber professionals. Security professionals now have a broad mandate for investigating and addressing online threats to the reputation of their company and its executives. Their employers and colleagues often seek their guidance in mitigating the many issues that result from the types of defamation, embarrassment and physical security risks that have become a common occurrence online. Today all major corporations and public companies have cyber departments within their security and investigations departments. The FBI has a cyber investigations unit, as do the law enforcement departments of most major cities.

SHORTCOMINGS OF CURRENT LEGISLATION

Passed in 1996, Section 230 has not been updated to accommodate the new platforms and new types of social behavior found online. It does not adequately protect individuals from defamation, from the widespread publication of their age and home addresses or from the harm that can result from both.

In the absence of legal protections, there are a range of strategies individuals and companies in the U.S. can put in place to safeguard their reputations online. This paper gives an overview of the leading online reputational threats, as well as an explanation of how such events unfold, the motivations behind them, and ways they can be protected against and resolved.

Before explaining these strategies, it is important to clarify what online reputation management is, how it differs from reputation management (which addresses corporate culture rather than Internet content) and how the aggregation and social sharing of information on the Internet contributes to ORM issues.

THE ONLINE REPUTATION MANAGEMENT INDUSTRY

The online reputation management (ORM) industry first appeared in the mid-1990s. From that point, it has grown in step with the Internet. ORM is popularly known as a service that repairs reputational damage caused by malicious anonymous commentary posted on Internet sites. Some ORM firms claim to improve reviews of businesses online (on sites such as Yelp). Others promise to push unwanted Internet content onto lower pages of search results. But the field is much broader, and the best firms use a range of techniques to protect and build a client's brand. A range of such companies can be viewed by Googling "online reputation management" and scanning the first five pages of results.

Like the Internet as a whole, the online reputation management business is largely unregulated. As a result, instances of extortion by disreputable ORM providers have been well-documented in the media (Krause, 2014). (For instance, any individual who has been arrested may be approached by an ORM provider that offers to control the dissemination of a mug shot. If the provider isn't contracted, it may disseminate that mug shot itself.) (Connelly, 2012)

Some ORM providers offer marketing services. They use a combination of content, technology and SEO (search engine optimization) to influence where a company's marketing materials appear in search results. The effectiveness of this approach can be impeded by the continually evolving algorithms Google and other search engines use to determine how results are ordered. (Visit Google's "How Search Works" for more information, http://www.google.com/insidesearch/howsearchworks/thestory/)

REPUTATION MANAGEMENT

Online reputation management is often confused with "reputation management," which refers to the broader task of maintaining the public integrity of an organization or individual's brand. Reputation management has exploded as an industry during the last ten years because of the rise of social media and the transparency it engenders, as well as the increased ability of citizens and consumers to comment publicly on behavior, policies and products. In addition to encompassing communications and public relations (including crisis management), reputation management is also a lucrative consulting practice that spans the review of every aspect of a company's internal structure to ensure its culture and practices adhere to and reflect a company's values (which includes best-practice management and procedures).

COMMON ONLINE REPUTATION THREATS FACING U.S. COMPANIES

Examples of online reputation threats that are commonly experienced by companies and organizations in the U.S. include:

- Public databases publishing executives' home addresses and information on family members. Once this information appears on one database, it is often harvested and disseminated through other outlets. This is not just a privacy issue; it can pose security risks as well.
- Publication of privileged emails and internal company documents that were leaked by inside sources.
- Organized online defamation campaigns.
- Being the subject of domain squatting: Registering or using a domain name ("[your name].com"), then offering to sell the domain to the person or company who owns the trademark at an inflated price.
- The impersonation of executives on social media and other online platforms. This can be a particularly damaging offshoot of domain squatting. It can be prevented by reserving appropriate handles in major social media platforms. Donald Trump was the subject of such an attack, and successfully sued for removal of the websites. (Draznin, Haley, 2014)
- Targeting of family members who have shared (perhaps too much) personal information on social media outlets.
- Being the subject of parody websites that criticize and lampoon CEOs and other public figures.

As a specialist working in this field, I have encountered each of these threats. I have seen emails from top executives at public companies get extracted from the company's secure digital archives and published in online forums; organized Twitter campaigns sending out multiple Tweets daily with links to defamatory false content about public figures; satellite photographs of the homes of high-profile executives published online with maps and directions to their homes and messages for readers to do them harm; and nude images of executives posted on multiple websites and social media platforms prior to a quarterly earnings release. Such cases are not usually publicized.

Common sources of threats include retaliation from severed business, social or personal relationships (most often dissatisfied or dismissed employees), but also competitors, industry bloggers who will benefit from the attention they receive, unhappy customers whose attempts to assuage their complaints through company channels have failed, individuals or groups with different political or social views, or simply anonymous "trolls" (people who cultivate discord on the Internet by posting inflammatory, extraneous, or off-topic messages in an online community).

Some threats can propagate online for months before being noticed. Most start on lower pages of Google and can take weeks to rise to a prominent position on page one of a Google search. Often company leadership becomes aware of them only when a crisis point is reached and it threatens to disrupt a brand or an individual's credibility.

Cyber security experts are often turned to in such situations. The communications departments of some companies, or executives charged with managing a firm's reputation (a growing practice), are also resources used to mitigate such issues. In some cases CEOs or another C-Suite executive ask their security directors to conduct an investigation to unearth the identity of the perpetrator. Forensic cyber investigators,

which growing numbers of law firms and investigative companies employ, can often identify the individual responsible for posting defamatory and other inappropriate content online. In some cases they partner with cyber specialists in law enforcement, particularly when they have relationships with that sector due to prior employment with Federal agencies such as the Secret Service or F.B.I. However, not all such posters can be easily identified.

It can be difficult to locate legal information sufficiently informative to indicate whether an online reputation issue meets the legal requirements of "defamatory" that are necessary to take legal action. Not all companies (or individuals) want to take such public action, either. An example of one successful lawsuit occurred in 2013, when a Harvard graduate was charged with online fraud, impersonation and harassment.(Leland, John, 2013)

One useful reference source for Internet legal information is the Chilling Effects Clearinghouse, a joint project of the Electronic Frontier Foundation and Harvard, Stanford, Berkeley, University of San Francisco, University of Maine, George Washington School of Law, and Santa Clara University School of Law clinics. This excerpt from their website explains their point of view:

> Chilling Effects aims to help you understand the protections that the First Amendment and intellectual property laws give to your online activities. We are excited about the new opportunities the Internet offers individuals to express their views, parody politicians, celebrate their favorite movie stars, or criticize businesses. But we've noticed that not everyone feels the same way. Anecdotal evidence suggests that some individuals and corporations are using intellectual property and other laws to silence other online users. Chilling Effects encourages respect for intellectual property law, while frowning on its misuse to "chill" legitimate activity. (www.chillingeffects.com)

Their extensive Boolean-format database provides quick searches of an exhaustive range of topics. The Electronic Frontier Foundation's website also has substantial information about Internet legal rights. (www.eff.org) This is an excerpt from its Bloggers' FAQ on Online Defamation Law, found in its Legal Guide for Bloggers' section:

> What is defamation?
>
> Generally, defamation is a false and unprivileged statement of fact that is harmful to someone's reputation, and published "with fault," meaning as a result of negligence or malice. State laws often define defamation in specific ways. Libel is a written defamation; slander is a spoken defamation.
>
> What are the elements of a defamation claim?
>
> The elements that must be proved to establish defamation are:
>
> 1. a publication to one other than the person defamed;
>
> 2. a false statement of fact;
>
> 3. that is understood as
>
> a. being of and concerning the plaintiff; and
>
> b. tending to harm the reputation of plaintiff.
>
> If the plaintiff is a public figure, he or she must also prove actual malice.

Google Executive Chairman Eric Schmidt and Google Ideas Director Jared Cohen address issues of defamation and privacy in The New Digital Age: Reshaping the Future of People, Nations and Business (Knopf, 2013):

> Smear campaigns and online feuds typically involve public figures, not ordinary citizens…our ability to influence and control how we are perceived by others will decrease dramatically.…The shift from having one's identity shaped off-line and projected online to an identity that is fashioned online and experienced off-line will have implications for citizens, states and companies as they navigate the new digital world….Identity will be the most valuable commodity for citizens in the future, and it will exist primarily online. (Schmidt, E., Cohen, J., 2013, pp. 32-36)

DATA SCRAPING RESULTS IN SERIOUS PRIVACY INVASIONS

Data scraping – the automated collection, indexing and publishing of online data– results in vast amounts of personal information about millions of individuals being available in "people" databases like Intelius and Spokeo, which package and sell it for nominal amounts ($10 or less). Many people, including high-profile targets, do not even realize their home addresses, ages and family members' names are widely available on such sites. But it can lead to serious physical security risks.

CONCLUSION

The best tactics for avoiding many of those crises are proactive. They include online monitoring of the company's and executives' online presence, as well as social media sites maintained by executives' family members. Numerous social media monitoring companies now provide such services, and Google alerts can be set up (for free) to monitor any keyword. (Due to a potentially high volume of daily alerts that may come into email boxes, setting up a designated email address just to receive alerts is recommended.) Company executives in particular should be made aware of online security practices, including protecting their data, using encryption for online correspondence and ensuring they avoid letting emails sit in their Gmail and other personal email boxes. Such emails are not only hacking targets, but can lead to the type of career-ending crisis as happened to General Petraeus. VIPs, including industry leaders, should place their real estate holdings in private trusts and buy any new properties through those trusts, which will help keep their private addresses from publicly available databases.

The most important tool for protecting against reputational crises is establishing a strong online presence. For companies, this should include forums where company representatives interact directly with customers to address grievances. Statistics show that the more options consumers have to air grievances in online settings provided by organizations, the less likely they are to vent in public forums, which can produce viral (and possibly justified) rants.

Effective planning can protect a company against many reputational threats. Reactive ORM techniques are increasingly focused on the production of quality content. The manipulation of search engine results—what used to be considered the central activity of ORM firms—cannot be guaranteed as search engine algorithms have grown more sophisticated and are continually being updated.

The best policies integrate strong security measures with a strategic and ongoing engagement with the Internet. Building a strong and authentic online presence not only allows a company to avert or respond to reputational crises; it is also a very effective way to build a brand and relationships with customers.

REFERENCES CITED

Connelly, Christopher (2012, December 23). Mug Shot Websites Charge When You're Charged, For Now. NPR. Retrieved from http://www.npr.org/blogs/thetwo-way/2012/12/23/167916738/mug-shot-websites-charge-when-youre-charged-for-now

Draznin, Haley (2014, March 2). Trump awarded damages in 'cybersquatting' case over domain names. CNN. Retrieved from http://www.cnn.com/2014/03/01/studentnews/trump-cybersquatting-lawsuit/

Krause, Kevin (2014, March 27), Former Texas resident charged with extortion for threatening to destroy client's online reputation. *The Dallas Morning News.* Retrieved from http://crimeblog.dallasnews.com/2014/03/texas-man-charged-with-extortion-for-threatening-to-destroy-a-former-clients-online-reputation.html/

Leland, John (2013, February 16). Online Battle Over Sacred Scrolls, Real-World Consequences. *The New York Times.* Retrieved from http://www.nytimes.com/2013/02/17/nyregion/online-battle-over-ancient-scrolls-spawns-real-world-consequences.html?ref=nyregion&_r=1&#comments

Schmidt, E., Cohen, J. (2013). *The New Digital Age: Reshaping the Future of People, Nations and Business.* New York: Knopf.

SHANNON M. WILKINSON is founder and CEO of Reputation Communications, which provides online reputation management services to CEOs, industry leaders, the C-Suite, VIPs and their organizations.

Contact: **sw@reputation-communications.com**
www.reputation-communications.com