



They've got their eyes on you—are your ears burning?

By: Briony Smith

ComputerWorld Canada (25 May 2007)

COMMENT ON THIS ARTICLE

At any given moment, your company's name could be dragged through the mud on the Web, as legions of bloggers, forum-posters, consumer grippers, and even your own coworkers mouth off on exactly what they think about your company, your wares, your competitors—even you.

To combat the millions of chatterboxes that comprise the "weblic," enterprise companies are now hiring online reputation management firms to keep tabs on what the denizens of the Internet are saying about them and their products. And, surprisingly, internal IT is often being left out.

Milton, Ontario-based CoreX Technologies produces RepuTrace, a proprietary software program, combined with human monitoring. "It's an all-in-one corporate intelligence tool that searches blogs, forums, message sites, consumer sites, gripe sites, and multimedia outlets," said vice-president of technology Joseph Fiore.

It is a Web-based system like a digital dashboard; an automated layer grabs information, which is then analyzed and reviewed by human monitors. Companies can choose a variety of alert methods, from automated e-mails to phonecalls for the urgent messages.

They can also log in to the company's Web page to check up on their updates. "Most of the reporting is done real-time in the product, on the fly. RSS feeds are on the site," said Fiore. All the information is stored on CoreX's own servers. IT staff do not have to manage the information in any way, according to Fiore.

The information that companies are after ranges widely, from tracking product sentiment to animal rights activists' posting board members addresses online. Some use it to check up on employees. Examples that RepuTrace has come across include employees discussing internal theft, badmouthing the business or its employees, disclosing proprietary company information, and talking about being drunk or high on the job. The company also recently identified a blog post where an employee threatened to go on a killing spree in their workplace.

"The Internet is definitely having an effect on employment law," said Bob Yeager, a lawyer in Vancouver, British Columbia. "People who are fired express surprise, figuring what is said here, stays here. But it goes everywhere!"

The software can also be used to track brand names and products to see where they stand in "weblic" opinion. Visible Technologies, a Seattle-based online brand management firm, makes TruCast, a Web-based enterprise software solution that searches social networks and pulls back information in real-time and scores it positive, neutral, or negative. Blake Cahill, vice-president of corporate marketing, said that the unique part of its offering is its response manager, which can allow the company to engage directly with a blog poster or someone writing in a consumer forum or social network, like MySpace or Facebook.

Indeed, the information collected is rather valuable, and creates opportunity for an integration of the information with business intelligence systems. Fiore said that the RSS feeds from Reputrace's module can be integrated with sales automation tools. "It's flexible enough to work with any system out there," he said. Again, IT would not be needed, though, to integrate the two systems. Visible Technologies has been called upon to integrate the information into an existing feedback mechanism as well.

Plus, the advent of RSS and the growing popularity of Web-based applications are easing integration between business intelligence systems and incoming information, according to Fred Palermino, CEO of Los Angeles-based Web optimization and online reputation management firm Lancer Media, who said, "It's getting easier for systems to talk to one another."

Such a feature could boost an ROI that might seem intangible. As Fionn Downhill, CEO of Phoenix, Arizona-based search engine optimization and online reputation management firm Elixir Systems, said, there has been very little data to prove the concrete ROI from online reputation management.

But, as Cahill points out, "It's like one huge focus group."

"One of the strongest ROI's is the quality of information and how it can be leveraged in different business units. It costs half of what a junior researcher would cost. The Canadian side of the PR profession is dialed in and wants to monitor—they see the damage it can do in a short amount of time. Part of it is that we understand the Web culture a little bit better," said Fiore.

Despite the IT department's general lack of involvement in these issues, they might still be called upon to help. Security breaches are becoming more and more common—if a breach occurs, the IT department could be the liaison between the company and the online reputation management firm, telling them what leaked information to keep an eye out for on the Web.

The line between the IT department, the marketing and PR crew could also become increasingly blurred, bringing IT into the online reputation management sphere after all. "As marketing goes online, you have to be interactive. To enable and empower the brand, marketing will more and more enter the realm of IT—it's a very great skillset (for IT professionals to have). Companies need someone who understands the marketing goals and what the application enables," said Cahill.

COSTS: RepuTrace: \$350-\$950 per month (higher prices for human monitoring hours) Visible Technologies: \$200,000 for monitoring one to two brands, to several million dollars to monitor many, per year

Rep management can cause a Big Brother backlash

Joseph Fiore, vice-president of technology for Milton, Ontario-based online reputation management firm CoreX Technologies (which produces RepuTrace software), acknowledged that some people see these technologies as invasive or an impingement on their freedom of speech.

Said Stephen Anderson, CoreX Technologies vice-president: "Anytime anyone gets terminated, they're gonna complain about it. It isn't a privacy issue — you wouldn't go into your boss' office and say those things."

Fiore said, "It's still new, so there's a reactionary aspect to it. People know you shouldn't get drunk at a company party and badmouth your boss, but people see the Internet in a different way."

Bob Yeager, an employment lawyer in Vancouver, British Columbia, said that employees can't really have an expectation of privacy when it comes to the Internet — but they can expect that employers won't take extreme steps to monitor them. Examples of this includes busting into log-in-only sites like Facebook (as Seattle-based online reputation management firm Visible Technologies does, courtesy of the Response Manager feature of their TruCast software). "In this case, the employer is acting predatory. It's like putting cameras where employees wouldn't expect them, and judges don't like that. Hacking into sites is where you get into trouble," said Yeager.

Blake Cahill, vice-president of corporate marketing for Visible Technologies: "It's like in customer service: if no-one answers the phone, nothing would get better. Why wouldn't companies want to engage? Some participants might not want the engagement, but a lot do want it. If they didn't want to be heard, they wouldn't say anything."

But they'd better watch their mouths: Yeager said that firing an employee for slanderous remarks against the company, revealing confidential information, or anything else that would get someone fired offline, is fair game.

Inside job

CoreX's RepuTrace software has come across some doozies.

And some of the time, the online reputation threat comes from within:

- A Fortune 500 employee threatened on their blog to "go on a killing spree" and burn down their workplace.
- Employees (including the grounds crew of a major airline) talked about being drunk or high on the job. Another incident found three employees discussing their drug and alcohol consumption on the job; when the company investigated, two out of the three had already been fired. The other one? The company owner's son.

Employees have:

- Reported on workplace safety hazards, using a forum to discuss dangerous equipment being used at work.
- Discussed workplace thefts they had committed (RepuTrace has monitored resale Web sites for the missing

merchandise).

- Revealed proprietary or confidential information.

Said Stephen Anderson, vice-president of CoreX Technologies: "We used to shake our heads at what we found, but we don't anymore—it's just too outrageous."

COMMENT ON THIS ARTICLE

Copyright © 2007
ITworldcanada.com