

Hundreds of keywords suggested to aid your surveillance of staff e-mails

We've already established that the **SEC** doesn't require that you monitor e-mails or search firm e-correspondence to detect risks and potential wrongdoing but it's certainly a best practice to conduct some e-eavesdropping ([IA Watch](#), July 25, 2011).

Most firms turn to keywords or phrases and use technology to periodically turn up instances where the language appears in their e-mail database. We solicited from your peers their favorite keywords and phrases and they responded, producing a [list of 348 words](#), ranging from "absolute" to "you told me."

The key is to "shave that [list] down to about 15 words," counsels **Bart McDonald**, executive VP of **Renaissance Regulatory Services** in Boca Raton, Fla. "Otherwise, you're going to get so many hits you won't be able to look through it."

False positives can dishearten a compliance officer when countless flagged e-mails fail to expose any smoking guns, says **Greg Florio**, co-managing partner at **Orical** in New York.

One CCO tells us he dropped omnipresent keywords like "buy" or "sell" in favor of phrases such as "call me at home" or "cell phone." Software can be programmed to skip words found within standard e-mail disclaimers or correspondence sent to a distribution list. Your effort should match the size of your firm and its risks. For instance, an extremely small firm in which the partners sit next to each other may not justify e-mail surveillance – but it certainly should retain e-

mails. SEC examiners likely will ask for them, says Florio.

"If you're not monitoring [e-communications], you don't know what's going on in your firm," believes **Peter Maftciu** of **Sound Compliance Services** in Gig Harbor, Wash. But you could limit your search to key individuals to save time, he says. Usual suspects include executives, portfolio managers, research analysts and sales and marketing staff.

Target 'high-risk employees'

Janaya Moscony, president of **SEC Compliance Consultants** in Philadelphia, agrees. Make it a point to look at your "high-risk employees," she says.

Another CCO found the exercise of opening flagged e-mails a tremendous waste of time and dumped the process in favor of spending one hour each Friday trolling through one person's e-mails and following the trail of conversations through the previous week.

"We have a lot of clients that will do both," says McDonald, of keyword and random searches or a combination.

False positives also drove **Paula Bosco**, managing director/CCO at **New Mountain Capital** in New York, out of the business of pre-populated keyword searches.

Instead, each quarter she looks at investment and business completed by her hedge and private equity funds and searches for keywords related to the recent deals. "It's always tied back to the business activity," she says. This way, the keywords are constantly changing.

IAWEEK

A publication of IAWatch

INSIDE...

More Guidance on Use of Social Media	3
SEC v. Judge Battle Carries High Stakes	3
Examples of Keywords for E-Searches	4
Arbitration Change Means More Courts	6

January 23, 2012

Four techniques employed

Aaron De Angelis, CPA/CCO at Spring Mountain Capital (\$620M in AUM) in New York, slices his program into four techniques. The first randomly applies keywords to 15% of all e-mails. The second method, also applied to another chunk of 15% of e-mails, examines the correspondence of key staff (e.g., portfolio managers, traders, sales people and executives). Another 30% of e-mails are simply randomly flagged. The fourth piece subjects the remaining 40% of e-mails to phrase searches, for instance, for “great performance” or “guaranteed performance.”

Exams and e-mail surveillance

Spring Mountain emerged from a 2009 SEC exam without any comments about its e-mail surveillance, says De Angelis. Indeed, he provided examiners with limited log-in privileges that permitted them to search e-mails using his system to flag any ones that they wished to ask about.

An even dozen exams have consumed Florio’s time in years past. In none of these, did examiners ask for the method the firms used to surveil e-mails. However, examiners do spot-check to confirm that you do what you say you’re doing, he cautions. They also may conduct their own keyword searches within a registrant’s e-mail database. Usually examiners request the entire e-mail box for senior officials within a given period of time, Florio adds.

Be sure to change keywords based on events. For example, should **Apple** stock soar through the roof, you may wish to search recent e-mails for “Apple,” says Florio. When he worked in-house, Florio would review each month the complete e-mail box for a given

person for the previous four weeks using a limited number of keywords. “I did it alphabetically and rotated it quarterly” to hit everyone over time, he says. You also could search for individual names, too, he suggests.

Some CCOs conduct their searches on a weekly, monthly or quarterly basis – often determined by their firm size and its risks, says Maftciu.

Usually firms, depending upon size, take a random sampling of 1% to 2% of their e-mails over a certain time and apply a keyword search, says McDonald. “You want to be reasonable” and not overdo it, he says. Firms engaging in riskier activities, such as investment banking, research or use of expert networks, may wish to step up such surveillance, McDonald says.