BAS
BOARD ADVISORY SERVICES, INC.

Counter Espionage Task Force Vs. A Sound Whistle Blowing Policy

by Laraine Terrell

Julian Assange: Folk Hero or Criminal?

I would argue that it doesn't matter; for better or for worse, WikiLeaks has changed the corporate world.

Take, for example, his effect on Bank of America. In an interview Mr. Assange said he had a hard drive containing information that, once exposed, would "take down a bank" and reveal an "ecosystem of corruption." The words "Bank of America" never even passed his lips.

And yet Bank of America executives leapt into action. According to the *New York Times,* the bank established a counter espionage team of 15 to 20 top officials, and brought in outside (and presumably expensive) resources from Booz Allen Hamilton and several leading law firms.

All at a time when the mind-share of the bank's top officials and outside resources would probably be better spent focusing on its marketing, customer retention and growth strategies. (Did somebody say lost revenue opportunities?)

Listen up Corporate America: To the disgruntled whistleblower, WikiLeaks means action. Julian Assange has become the go-to man for potential whistleblowers who fear reporting wrong-doing through their company's official policies.

Jay Simmons, Co-Founder and Chairman of Board Advisory Services, couldn't agree more. "This country has seen a legislative push toward creating an open and ethical culture in business, one where employees can report wrongdoing without fear. Congress has dictated specific requirements to establish processes to achieve such a culture. And yet all of these efforts have failed miserably. In such a climate, a WikiLeaks becomes inevitable."

Pity the Whistleblower

Ten years ago, several horrendous corporate malfeasance scandals toppled mighty corporations. Responding to public outcry, the U.S. Congress enacted the landmark Sarbanes-Oxley, ushering in new era of transparency. One of its provisions required all companies to establish and communicate to employees procedures for reporting wrongdoing, as well as policies that prevent retaliation against anyone who comes forward.

In spite of SOX, whistleblowers are not protected, and retaliation is all but certain. Last summer my company was approached by a whistleblower who had reported a serious regulatory breach to the risk and compliance officials, only to be shut out and eventually ruined financially. Meanwhile, the CEO makes speeches about the importance of transparency, compliance, and honest behavior.

Unfortunately, focus is still on smearing the whistleblower rather than looking at the issue. But the company loses when whistleblowers fear for their jobs, careers and life savings, because instead of having serious issues flow up to the CEO and Board where they can be addressed early and quickly, Mr. Assange has offered up his website and services.

Fixing the Corporate Whistle-Blower Policy

Not too long ago, my company Board Advisory Services (BAS) reviewed the reporting, whistleblower and non-retaliation sections of the Codes of Conduct of some 100 companies in a wide array of industry sectors. Our conclusion: with a few notable exceptions, most are abysmal.

It's worth pointing out that in nearly all instances, we located the company's Code of Conduct in its Investor Relations section of its website. Clearly, Chief Risk Officers and the Chief Legal Counsel view the Code of Conduct as a critical safeguard meant to assure potential investors (and ratings agencies) that the company takes ethics seriously. In other words, a Code of Conduct is proof-positive of an ethical corporate culture, and a safe place to invest one's money.

But a Code of Conduct should be more than a checklist item on a website. It should be a vibrant, relevant document, one that guides and inspires employees to act ethically. Why aren't they? Below are some of the issues we've discovered.

Boilerplate Code of Conduct

Far too many of the Codes of Conduct we reviewed are boilerplate documents, with the company's name appearing only on the title

page. Many didn't even bother to change "The Company" to the name of their own enterprise. Only a few took the time to write their Code of Conduct in terms that are meaningful to their employees.

It's a mistake not to customize the Code of Conduct to the conditions facing a specific company or, at a minimum, its industry. Surely the circumstances that can give rise to violations in a Code of Conduct for financial services professionals are significantly different from those facing healthcare or consumer marketing professionals.

For many employees, the boilerplate language used in their company's Code of Conduct can be so abstract that it bears little relation to their daily work lives. That, in turn, negates the importance that a Code of Conduct should inspire in employees, and does absolutely nothing to guide their behavior.

Call It a Whistleblower Policy

Less than 10% of the Code of Conduct documents we reviewed contained the term 'whistleblower.' Why is that the case, when a well-designed whistleblowing program encourages people to bring unethical or illegal activities to management's attention so they can address potential problems before they're sent to WikiLeaks?

By adopting an official whistleblower policy – and naming it in the Code of Conduct – Chief Risk Officers will provide the encouragement employees need to come forward when they have an urgent matter to report.

Reporting through Chain of Command

The vast majority of Code of Conduct documents we reviewed instruct employees to report violations to their supervisor, or to their supervisor's supervisor if their immediate manager is the source of the problem. If the employee isn't satisfied working through the chain of command, many companies offer their HR department or the chief legal officer as a next step. Some, almost grudgingly, offer reporting via a third party, but only as a last resort.

How should ethics violation be reported?

The best way to encourage reporting is to engage the services of a third party and to make that outside resource the first – not last – point of contact for the employee. Take care to select a vendor who can receive the complaint anonymously; solicit supporting documentation and other proof points needed to test the veracity of the complaint; follow up with the employee filing the complaint while maintaining his or her anonymity; and provide the CEO with a list of all the complaints that have been received, and the status of the investigation on a regular basis.

Reporting directly to the CEO may seem a bit cumbersome, but it is the only way to ensure that no layer of management is able to participate in a cover-up or engage in retaliation. Using a third party to test the veracity of complaints by soliciting supporting documents and other proof-points from the employee will save the chief risk officer from wild goose chases.

Toothless Non-Retaliation Policies

All of the Code of Conduct documents we reviewed stated that it is the company's policy to prevent retaliation. Unfortunately, that's pretty much all that was said on the topic.

Perhaps one can easily assure an employee that he or she will not be terminated for reporting a violation. But retaliation often occurs in much subtler ways, such as excluding a whistleblower from meetings where new initiatives are discussed and ownership is assigned. How does a chief risk officer prevent a whistleblower from being sidelined? Can a policy monitor and mitigate that risk?

The truth is, good intentions are not enough to guarantee non-retaliation. That's why it's so important that the policy guarantee confidentiality.

In conclusion, the best way for companies to prevent their memos, emails and documents from ending up on WikiLeaks is to establish meaningful whistleblower policies; ones that embrace the spirit, and not just the letter, of the law. That policy should include creating and disseminating Codes of Conduct that are meaningful to employees and guarantee non-retaliation by using a third party to receive and vet complaints.