An ALM Website

January 10, 2011

CORPORATE COUNSEL

To Preserve and Protect: Warding Off Wiki-Like Attacks

Sara Jane Shanahan

Companies and investors have been monitoring recent news reports regarding the defensive actions that Bank of America has taken following statements in late 2010 by WikiLeaks founder Julian Assange that he intends to "take down" a leading American bank and that WikiLeaks has a hard drive from a Bank of America executive.

According to reports, Bank of America Corporation has launched an extensive internal investigation to determine both the source and the substance of potential information leaks. In addition to looking for recent data leaks, Bank of America appears to be reviewing materials related to regulatory and congressional investigations into its acquisition of Merrill Lynch & Co., Inc., and mortgage loans made by and acquired from Countrywide Financial.

The bank's objective is to uncover the allegedly damaging materials and prepare a legal and communications response in advance, rather than reacting in real-time

Sara Jane Shanahan

if and when WikiLeaks makes its next disclosure, which is rumored to be planned for early this year.

What lessons can other companies learn from Bank of America's predicament? Three areas for preemptive action stand out — know your technology, cultivate your human capital, and update your internal audit programs.

Know and secure your technology. The recent and prolific disclosures by WikiLeaks have only highlighted what companies have known for some time now — the emergence of e-mail, BlackBerrys and other smart phones, easily accessible storage sites in the "cloud," and simple flash drives has made it very easy for employees to transfer large amounts of internal corporate documents and data to competitors or others who might wish your company ill, such as WikiLeaks or another entity similarly interested in making a name for itself by publicly disclosing embarrassing or damaging documents.

Information technology specialists should be consulted for advice on the most current anti-theft techniques. For example, issuing password-protected BlackBerrys for corporate use to employees allows a company to shut down a device if it is lost or stolen and to delete data stored on the device on a routine basis.

Updating an inventory of computer systems used or otherwise maintained company-wide can also protect against disclosures from "forgotten" caches of data. After an acquisition, the new parent company should take time to identify and secure newly acquired systems. Structuring your computer-based and hard-copy files such that individual workers or departments cannot access documents outside their area of operation can limit the number of potential leakers.

Build, don't burn, your bridges. With the unemployment rate hovering around ten percent, it is a fact of modern corporate life that people will lose their jobs. In addition, corporate insiders, especially in the pharmaceutical and financial industries, are facing conflicting loyalties in light of newly enacted government bounty programs that promise hefty payoffs for whistleblowers.

Against this backdrop, investing in outplacement services for displaced workers and internal training programs that encourage employees to report issues of concern to internal audit or compliance departments can assist companies in heading off leaks that are intended to harm the company or somehow benefit a disgruntled employee.

Training employees to exercise common sense and discretion when writing e-mails and using social media can also reduce the volume of potentially embarrassing documents that someday could be leaked. Leading by example is a low-cost and high-yield management tool — if the boss refrains from sending "strongly worded," disparaging, or otherwise unprofessional e-mails, the sales team or work force at large is more likely to exercise similar restraint.

Audit your internal audit function. While Assange has hinted that he may release information potentially harmful to Bank of America, not every company will receive advance warning of a "wiki-like" leak.

Accordingly, public and private companies alike should review their internal audit and compliance programs and determine, before a leak or a warning occurs, if current procedures address the risks associated with intentional and unauthorized disclosures of internal documents.

Harmful leaks will come in varying forms — disclosure of competitive information such as key pricing or other deal terms, disclosure of damaging information that exposes the company to liability, or disclosure of embarrassing information that reveals a corporate leader's exercise of poor judgment.

In the aftermath of high-profile thefts of consumer credit card data from retailers, companies throughout the retail industry took immediate steps to review and improve the security measures used to protect consumers' financial and identifying information. After recent disclosures of improper foreclosure practices at high-profile banks, banks across the country have undertaken to examine their own practices, without waiting to receive a subpoena from a state or federal investigator.

Similarly, the recent disclosures by WikiLeaks — ranging from diplomatic communications to internal corporate information to old-fashioned embarrassing e-mails — should prompt companies to implement updated procedures designed to prevent and detect unauthorized disclosures of sensitive materials.

With the Super Bowl approaching, companies would do well to heed the old football adage — the best defense is a good offense. Such affirmative steps can help companies prevent unauthorized disclosures and respond proactively, rather than reactively, when leaks do occur.

Sara Jane Shanahan, a partner in the Litigation Department of Sherin and Lodgen in Boston, focuses her practice on complex business litigation and insurance coverage disputes. She can be reached at SJShanahan@sherin.com.