

# CORPORATE COUNSEL

## Lessons Learned From WikiLeaks: Don't Be a Target

*Heather Egan Sussman and Obiamaka P. Madubuko*

Every in-house lawyer is now familiar with the WikiLeaks story.

The organization claims to provide a safe haven for whistleblowers and for the public dissemination of private information, with a self-proclaimed goal of assisting "peoples of all countries who wish to reveal unethical behavior in their governments and institutions." During 2010, WikiLeaks posted to the public domain hundreds of thousands of classified documents from the U.S. government and military.

These leaks have left many government officials scrambling to perform damage control.

Despite a clear focus on government in 2010, WikiLeaks is expected to turn its attention to the private sector in 2011.

Recently, *Forbes* interviewed WikiLeaks founder and front-man, Julian Assange. He claims that half of the information that WikiLeaks is currently sitting on involves private corporations.

Early next year, WikiLeaks reportedly plans to make public detailed information about at least one major American bank that, according to *Forbes*, will "lay bare the finance firm's secrets on the web for every customer, every competitor, every regulator to examine and pass judgment on."

In light of this chilling forecast, there are concrete steps in-house counsel can take to avoid having their companies' confidential data leaks become front-page news.

### GET YOUR HOUSE IN ORDER ON THE DATA SECURITY FRONT

Many in the corporate world think their data will not be targeted by WikiLeaks because they have operated transparently

and maintained integrity in business dealings. All businesses should be concerned about leaks, however, because of the risk that a disgruntled former employee may release misinformation or a company's trade secrets and, at that point, the proverbial genie is out of the bottle.

An important lesson from the WikiLeaks story, therefore, is that all companies should have their houses in order on the data security front. This means in-house counsel need to step up to the plate, and no longer simply rely on IT departments to handle data security.

Instead, the legal department should appoint one or more lawyers (or trained privacy officers) to ensure IT security is integrated into a broader corporate privacy and data security program that addresses non-technical functions, such as administrative and physical security controls.

After all, a business can have the best firewall protection, but this does not prevent an employee from walking out the door with the company's trade secrets on a CD-ROM. Essential components of an effective privacy and data security program include measures that protect networks, equipment, data, and personnel.

To protect networks, in-house counsel should ensure they have a qualified specialist in charge of system security. The foundation of any effective security program is having adequate technical safeguards in place to control access to infrastructure and to monitor the flow of information in and out of the organization.

In-house counsel who want a crash course in how hackers steal data should read Hewlett-Packard Company's 2010

Top Cyber Security Risks Report. In-house lawyers should share this report with IT to be sure they have implemented the security controls suggested in the report.

Regarding equipment, most companies already have basic software controls like antivirus protection. In-house counsel should also evaluate the merits of hard-disk encryption and deploying equipment recovery software that can remotely track and wipe missing devices.

Effective hardware controls, such as inventory programs that keep track of computers and portable media, are also critical. After all, it is difficult to know when a piece of equipment has been lost or stolen without having a proper inventory. An effective inventory program also should dictate a procedure for decommissioning equipment that includes either destroying the equipment or permanently wiping all data.

Too many businesses have faced the horror story of a rogue IT employee selling unwiped equipment on the secondary market. That equipment can reveal sensitive information about a company that can end up in the hands of WikiLeaks, if not a competitor.

In-house counsel should also ensure they employ proper protections for data through a classification policy that puts information in classes like "public," "confidential," "personal," or "highly sensitive." Companies can then wrap physical (e.g., locked file cabinets) and technical (e.g., encrypted databases) protections around classes of data as needed.

In addition, data should be placed into categories, like financial data, trade secrets, sales data, employment data, and the like.

Internal access then can be restricted across data categories to enhance protection.

For example, an HR employee might have access to all classes of employment-related data, but only "public" financial data. Highly effective security systems also implement measures to detect whenever an unauthorized employee (or an outside threat posing as one) attempts to access data.

Finally, regarding personnel, some hackers use "social engineering" to target unsuspecting employees who can be duped into providing passwords and access to company systems or premises. In-house counsel can reduce these risks by implementing training programs to teach employees how to avoid common traps, and how to recognize red flags or suspicious behavior.

Of course, this does not always protect against inside jobs. In that case, it is critical to have in place good hiring practices that include conducting thorough background checks, vetting references, and requiring employees to sign clear, enforceable nondisclosure agreements.

## IMPLEMENT EFFECTIVE WHISTLEBLOWER PROGRAMS THAT ENCOURAGE INTERNAL REPORTING

Having a strong internal reporting system in place can also help to avoid a public disclosure scandal.

Companies should encourage employees to report concerns internally through a whistleblower program or other anonymous reporting method. Encouraging internal reporting is a hallmark of any effective compliance program, which is the first line of defense against unwanted leaks.

If an employee feels like their report will be taken seriously or can be made without fear of retribution or penalty, internal reporting becomes a desirable option. Having in place a strong anti-retaliation policy that protects whistleblowers who make good faith complaints also encourages internal reporting. Internal reports should be investigated promptly.

To create a robust compliance program, companies must set the tone from the top down. This includes having a strong code of ethics endorsed by senior management and establishing clear rules and enforcing them fairly and consistently.

Companies should recognize and reward compliance-driven individuals and include compliance-related goals in reviews and compensation decisions. Rewards may be monetary, or they can include recognitions, intangible benefits, and additional perks such as days off.

By using a set of carrots and sticks of financial or other incentives and by creating a culture of compliance, you can inspire your employees to become more compliant-minded, and to follow the rules and follow the law.

## ASSEMBLE LITIGATION AND MEDIA TEAMS AND CREATE A PLAN OF ACTION

For business with data already stashed in WikiLeaks' reported treasure trove, the age-old adage of "the best defense is a good offense" applies.

In-house counsel should consider assembling their litigation and media teams now to develop plans of action. Counsel should think ahead about litigation options. If an employee violates a nondisclosure agreement by publicly disseminating confidential information, possible remedies may include injunctive relief and claims for monetary damages based on breach of contract, fiduciary duties, or other grounds.

To obtain an injunction, a company generally must show: 1) a strong or substantial likelihood of success on the merits; 2) irreparable injury; 3) whether the injunction would cause substantial harm to others; and 4) whether the public interest is served by the issuance of an injunction.

If the information is published anonymously through a journalistic site, injunctive relief may not be possible in light of the prior restraint doctrine, which recognizes that the media has broad First Amendment rights that should not be abridged except for compelling circumstances.

Unfortunately for many corporate victims, risk of economic harm alone does not rise to the level of compelling circumstances. Depending on the jurisdiction, however, if a company can meet the elements for an injunction and further demonstrate that the other side acted in bad faith or knowingly obtained or, had reason to know, that the information was obtained illegally, some courts have permitted injunctive relief to the aggrieved party.

In addition, companies can prepare ahead for a data leak crisis by planning an effective media strategy: 1) determine what types of information may be released and how the company will be impacted by this public disclosure; 2) identify the stakeholders (e.g., employees, customers, and investors) and determine how to communicate with these stakeholders in the event of a public disclosure; 3) prepare a messaging strategy; 4) determine who will deliver the message and who the audience will be (e.g., using an attorney spokesperson or company executive); and 5) train all employees on how not to respond to a crisis (e.g., sending improper e-mails and how to be cognizant of the tone and content of all written communications including e-mail, text, and instant messages).

## CONCLUSION

An important lesson from the WikiLeaks story is that in-house counsel should no longer simply rely on IT departments to handle data security.

Instead, the legal department should ensure IT security is integrated into a broader corporate privacy and data security program that includes measures that protect networks, equipment, data, and personnel. In addition, in-house counsel can implement effective whistleblower programs to encourage internal, rather than external, reporting.

Finally, in-house counsel who are concerned that their company's data may be at risk of exposure should assemble their litigation and media teams now to develop a plan of action. Following these steps will help counsel plan for and navigate through the unexpected leak of confidential information in the public domain.

*Heather Egan Sussman is a partner in the labor and employment group of McDermott Will & Emery, and is co-chair of the firm's global privacy and data protection affinity group as well as a certified information privacy professional. She is in the firm's Boston office. Obiamaka P. Madubuko is a partner in the white collar and securities defense practice group at McDermott Will & Emery and is resident in the firm's New York office.*