How to Build Your WikiLeaks Wall

Publication
3.16.11

In November 2010, WikiLeaks' founder, Julian Assange, disclosed in a *Forbes* magazine interview that the organization's next target would be a major American bank. Assange's statement, and the subsequent public discourse, is an important reminder to all businesses about the necessity of preventative measures to protect disclosure or discussion of sensitive private information. Potential breaches of confidential information protection could be as informal as an employee's Facebook posting or a much grander disclosure of actual documents on a website.

It should therefore be a fundamental objective of every organization to implement policies and procedures geared toward protecting confidential information. Supplementing this information protection strategy is a social networking policy aimed at limiting/prohibiting use of social networking sites in the workplace, controlling the company-related information disseminated on these sites and entitling a company to monitor discourse on these sites when a company computer is used.

Implementing controls will certainly make it much harder for a current or departing employee to compromise a company's trade secrets. However, adverse actions taken against employees who engage in the improper data may be prohibited by certain state and federal anti-retaliation provisions. Employers should review the situation with Human Resources and

This article appeared in the March 16, 2011 issue of *Business Finance*.

Copyright © 2024 Fisher Phillips LLP. All Rights Reserved.