Open Source, Hidden Exposure

Publication
2.01.10

In an age when the ubiquity of computers has made the exchange of data effortless, a school of thought has emerged that suggests that "information wants to be free." Many computer programmers have taken this philosophy to heart with the creation and promotion of "open source code," computer programming language that by its very nature, is designed to be shared, at no cost and for no profit, by anyone who wants to use it. But what happens when open source aspirations come into conflict with the proprietary need to protect an organization's most vital trade secrets?

The context for understanding how an employee's use of open source code can impact a company's trade secrets begins with the unprecedented use of computers in the workplace. Today, ever-increasing numbers of employees are assigned individual work computers with internet and e-mail access. As employee use of computer systems has proliferated, so too has the use and movement of computer code, which consists of instructions given to a computer in order to make it perform tasks.

Companies need to take a proactive, comprehensive approach to determining and monitoring how their employees are using open source code and analyze the controlling licenses. This process will likely require collaboration between counsel, risk management, product/business development, human resources, information technology and employee supervisors. These necessary steps might appear costly, but are insignificant compared to the potential damage that could result from the loss of trade secret protections.

This article appeared in the January/February 2010 issue of *Risk Management Magazine.*

Related People

Brent A. Cossrow
Regional Managing Partner
610.230.2135
Email