Baton Down the IT Hatches When It Comes to Exiting Employees

By Eric Sinrod,

Companies apparently need to be afraid - very afraid - and must be very careful when dealing with exiting employees who have knowledge of corporate information technology.

Indeed, according to a recent survey by Cyber-Ark Software, as many as 88% percent of IT administrators, if laid off tomorrow, would abscond with sensitive company information. Such information includes high-level and privileged passwords, customer databases, R & D plans, financial reports, HR records and merger and
acquisition plans.

Privileged password lists are particularly problematical, as they provide the keys to unlock access to information residing on corporate networks. And of the group that said that they would abscond with company information, one-third stated that they would take the privileged password lists

Because of the danger presented by departing IT personnel who still might be able to access corporate networks, it is important to "secure passwords and related identities as much as possible. Furthermore, passwords should be changed regularly.

Perhaps not too surprisingly in this climate, one-third of companies revealed that they believe that industrial espionage and data leakage is commonplace. Such wrongful transfer of data can be accomplished by way of email, mobile devices such as USB sticks, iPods, Blackberry's, and laptops.

Also, one-quarter of companies conceded having experienced internal sabotage or cases of IT security fraud happening in the workplace. Frankly, the percentage very well could be higher, because this is something that many companies do not want to admit.

Layoffs are not uncommon these days, in this tough economic climate. While downsizing might be important, it is critical that companies take care when it comes to protecting information systems. It is no longer enough to simply walk an employee out the door. In addition, companies must take steps to ensure that a departing employee has not left with valuable company information and cannot gain further access to company networks.

Eric Sinrod is a partner in the San Francisco office of Duane Morris LLP (http://www.duanemorris.com) where he focuses on litigation matters of various types, including information technology and intellectual property disputes. His Web site is http://www.sinrodlaw.com and he can be reached atejsinrod@duanemorris.com. To receive a weekly email link to Mr. Sinrod's columns, please send an email to him with Subscribe in the Subject line.

This column is prepared and published for informational purposes only and should not be construed as legal advice. The views expressed in this column are those of the author and do not necessarily reflect the views of the author's law firm or its individual partners.