THE JOURNAL RECORD

Gavel to Gavel: Filling data security gaps

Sept. 17, 2015
By Tim C. Vincent II

Sound data security programs are not only structured, but populated. Managers provide active oversight of employee access to and usage of data. Proper management can help avoid certain often-overlooked security gaps.

• Incomplete identification of total access to information: Most reviews of employee access focus on hard access – what systems employees have been given access to via login or password. What's not always identified or controlled is soft access to information outside direct systems permissions. This includes hard-copy reports and information received through a "CC" on an email. Clear expectations regarding distribution of particular information, along with job descriptions identifying necessary access, can provide guidance to employees in advance of inappropriate sharing of such information.

• Inappropriate access following a change in position: When an employee begins work, access to various systems is typically provided based on an access authorization form. While initial access may be based on an employee's job at that point in time, position changes don't always result in appropriate access changes. If an employee moves from an internal to an external role, it's important that the previous access be revisited and revised to prevent inappropriate access to information that is no longer necessary for the current job. When an employee terminates, accurate documentation of current systems access is important to ensure that all access is shut off at the appropriate time.

• Unrealistic mobile device expectations: Many companies utilize a bring-your-own-device approach. Employees use their own laptop, phone or tablet for company purposes. Data security risks of such devices can be significant. Talking to potential hires about intended use of such devices may highlight some practices that should be monitored, or even changed, if someone is hired. Also, you may want to confirm that the recruit's laptop will work within your company's systems.

Data security has become yet another element of employee responsibility and performance to be discussed and reviewed, even before the employee is hired. Proper identification and management of expectations and access can provide a manager with greater confidence in the security efforts of both her subordinates and her company.

Tom C. Vincent II is an attorney with the law firm of GableGotwals and a former bank compliance officer. His practice areas include banking and financial services compliance and data security.