THE JOURNAL RECORD

Gavel to Gavel: Data security starts before hiring

By: Tom C. Vincent II Guest Columnist March 7, 2018

Tom C. Vincent II

Almost daily, we learn that yet another corporation has suffered a major data security breach, potentially exposing the private information of millions of people.

However, it's not always faceless, faraway hackers who are a threat to data security. Data can also be vulnerable due to employee error – which often results from not having a clear understanding of company policy.

As almost every company handles valuable data of some sort, security is an important responsibility throughout an employee's entire tenure with the company – even before a hiring. In the pre-hire process, data security requirements and responsibilities of both the company and the employee should be established, documented and communicated. During the interview process, human resources and hiring managers should communicate the expected data security protocols.

When a new employee joins the team, managers should ensure she receives information security training that is appropriate to her particular job responsibilities. Company policies addressing internal information classifications and required security, acceptable use of company technology and devices belonging to the employee, and incident reporting procedures should be provided and explained.

This includes training on appropriate data storage and movement, such as where to save sensitive information, what to leave in and remove from email, what can and can't be sent to and from personal email and how to properly send sensitive information.

When an employee leaves the organization, it is always a good idea to remind the employee of the company's data security rights and responsibilities. Given the transportability of data, the company may want to reinforce the departing employee's responsibility to "bring everything back/leave everything here" and obtain some certification that nothing has been taken.

Limitations on systems access (appropriate to the timing and nature of the departure) are also crucial. There should be a plan for dealing with personal information on company computers that includes human resources and IT (and in some cases legal) along with the terminating manager.

Finally, the employer should make sure the departing employee's technology is preserved in the event issues are identified later. This includes not reassigning a computer that may need to be reviewed because of potential difficulty in separating the new information from the old and the risk of the prior user's information being corrupted or deleted.

Tom C. Vincent II is an attorney with GableGotwals, a full-service law firm of more than 90 attorneys.

http://journalrecord.com/2018/03/07/gavel-to-gavel-data-security-starts-before-hiring/