Mark Wiletsky

Partner
303.473.2864
Boulder
mbwiletsky@hollandhart.com

Employees Hold the Key to Data Security

Employees Hold the Key to Data Security

Insight — 10/31/2007

It has become almost commonplace to hear that a governmental agency or private corporation has been the victim of a data security breach. As a result, hundreds of customers' or employees' personal data is at risk of being used for criminal purposes, such as identity theft. Approximately 70% of these breaches are caused by an insider. In many cases, a laptop computer containing sensitive information is lost or stolen from a car or home. Other times, someone hacks into a system containing confidential information.

In response to this steady drumbeat of breaches, a majority of states (39 and counting) have enacted "notification" laws. These laws are typically triggered when some combination of a person's unencrypted personal information (such as first and last name, address, Social Security number, and driver's license number) is compromised. The organization that suffered the breach must notify the individuals affected and, in some jurisdictions (*e.g.*, New York), state agencies. A breach may trigger notification laws in the state where the company does business, as well as the states in which residents have been or might be impacted by the breach.

In addition to state notification laws, there are industry-specific laws that regulate data privacy and security. For example, the Health Insurance Portability and Accountability Act (HIPAA) requires covered entities to safeguard protected health information of patients, and the Gramm-Leach-Bliley Act requires financial institutions to protect consumers' financial information. Even those in unregulated industries often maintain sensitive personal information concerning their employees, including Social Security numbers and medical records, *e.g.*, for workers' compensation claims, FMLA requests and requests for accommodation.

In light of this patchwork of laws and the ever increasing threat of experiencing a data breach, organizations can and should take some basic steps to keep their data secure and to prepare in advance for a breach. In developing safeguards for sensitive data, organizations should remember that employees are not only the most likely candidates for causing a security breach, they are also the best defense against such a breach occurring in the first place. The following steps for safeguarding sensitive data are by no means exhaustive, but they are a good starting point in the process.

Step One: Background Checks

Thorough interviews and background checks are critical to minimize the

likelihood of hiring someone who poses an undue security risk. Background checks may include, among other things, verifying employment history, and checking references and criminal records. The failure to properly screen an applicant would almost certainly be used against a company if the person stole information and had a history of such misconduct that was easily discoverable.

Step Two: Develop Appropriate Policies

Most organizations have handbooks that are distributed to employees. Handbooks should be regularly reviewed and updated to ensure appropriate data security policies exist and that they accurately reflect the current business model and technological advances.

In developing or updating data security policies, it is important to involve the right players, which typically includes a mix of people from management, human resources, information technology, and inside or outside counsel. Next, an organization should map out the key data in its possession so that it can analyze the legal requirements for security, who such information flows to, who has access to it, who actually needs to have access to particular aspects of the data, and so on. Finally, the policy must be developed, tested and implemented.

Data security policies have many elements, and they will vary depending on the nature and size of the business. Still, there are some common themes. In addition to a critical incident response plan (discussed below), a data security policy might cover: use of laptops (at home or when traveling) and other portable devices; password protection and encryption; data back-up and disposal procedures (be familiar with the disposal rules promulgated by the FTC pursuant to the Fair and Accurate Credit Transaction Act); data classification and access; e-mail and blogging; and limitations on downloading, printing and transmitting information, especially to third parties, home computers or other non-secure recipients.

Step 3: Create a Critical Incident Response Plan

Organizations should prepare a critical incident response plan before an incident occurs. The plan should identify a person or position responsible for receiving and investigating reports concerning data breaches. In light of the potential legal liability associated with a breach—which can involve criminal law enforcement, state or federal agencies, or an individual or a group of potentially affected persons—it is critical to involve inside or outside counsel as soon as possible to protect, to the extent permissible, communications related to the event under the attorney-client privilege.

Step 4: Supervision and Training

A data security policy that sits on a shelf gathering dust is not only unhelpful, a plaintiff would surely argue that the company's failure to follow its own policy amounts to negligence. Therefore, it is critically important to train and supervise employees so that they know and understand how to keep information secure and what to do if a breach occurs. Consider training employees on the policy during a routine orientation process and

as part of an annual review, or whenever the policies are revised or updated.

Step 5: Review Your Contracts

If a company contracts with vendors or other third parties to handle or process transactions or other information, be sure to analyze what kinds of safeguards they have in place to protect the confidential information to which they will have access. Employees should know what information they can, and can't, share with third parties. Another concern is what liability, if any, the vendors or the company will have in the event of a breach. It's better to address these issues at the beginning of the relationship, as opposed to after a breach has occurred.

There is no way to completely protect against a data breach, but a few simple steps can go a long way to minimizing the risk and potentially avoiding a lawsuit if a breach does occur.
