The Role of Personnel in Data Breaches and Cybersecurity Issues

Employee error is responsible for most data breaches. Non-malicious mistakes by employees in the form of: failing to lock a door, using the wrong email address, forgetting an electronic device on a plane or train, or forwarding the wrong attachment, lead to a majority of the data breaches that confound employers.

Indeed, data breaches are not limited to electronic data. About one in four data breaches involve paper or other non-electronic data.

There is an Illinois Law that Governs Data Breaches.

48 states have data breach laws and Illinois is no exception. Effective January 1, 2017, Illinois amended its Personal Information Protection Act ("PIPA") which expanded the definition of protected personal information and increased data breach notification requirements. Illinois' original PIPA statute became effective in 2012, and the Illinois Attorney General published a very useful guide to the statute and its notification requirements here.

Employee Training is the Most Effective Way to Counter Data Breaches.

Employee training is the most effective way to prevent breaches. Indeed, this has been codified into federal law and some state laws. For example, healthcare providers, health plans, and business associates are explicitly required to train their employees on privacy and security under HIPAA Privacy Rules. Financial institutions are required to train their employees under the Gramm-Leach-Bliley Act.

Illinois' amended PIPA requires all employers that collect protected personal information, and nearly all employers do, "[to] implement and maintain reasonable security measures to protect those records from unauthorized access, acquisition, destruction, use, modification, or disclosure." Employee training is one such reasonable security measure.

What Should a Training Program Look Like?

Data breach training should resemble safety training or harassment training. Generally, everyone in an employer's business should receive customized training based on their level of sophistication. At a minimum, employees should be taught what is confidential or personal information, and what is a data breach. Finally, training should be documented. This means that employers should be able to produce the training curriculum they used and they should record the names and dates of all employees who received training.

Cybersecurity Insurance As a Last Ditch Defense.

Even the best trained workforces will experience a data breach. For most businesses, a data breach may only be embarrassing and inconvenient. For those "black swan" events, however, insurance is a must.

Employers should price cybersecurity insurance that is primary, not merely an endorsement on their property and casualty policy. If available, a cybersecurity policy should cover pre-existing problems. Some insurers retain forensic experts for use in cyber investigations and employers should know if they are required to use the carrier's expert or if they can use their own. "Conduit coverage," which protects an employer if another entity it does business with suffers damages should also be considered.

Data breaches are bound to happen. The damage they do can be mitigated, however, by effective training and a reasonably priced insurance policy.

If you have any questions about the matters addressed in this *CCM Alert*, please contact the following CCM author or your regular CCM contact.

Ross I. Molho
Clingen Callow & McLean, LLC
2300 Cabot Drive, Suite 500
Lisle, Illinois 60532

www.ccmlawyer.com
(630) 871-2614

The author, publisher, and distributor of this CCM Alert is not rendering legal or other professional advice or opinions on specific facts or matters. Under applicable rules of professional conduct, this communication may constitute Attorney Advertising.