Legal Perspective: Are you liable if hackers steal your employees' data?

By Ryan Scharnell For TBLN | Posted: Tuesday, April 4, 2017 11:15 am

Ryan Scharnell

Scharnell

The question seems to no longer be if your company will be the victim of a data breach, but when.

As employers collect and store more of their employees' personal information, they became potential targets for hackers. If hackers steal sensitive employee data, employees may sue for damages caused by the use of that information.

Courts are just beginning to address the potential liability of employers in this situation and have reached differing conclusions.

Victimized employees generally seek redress in negligence from their employers. Under a negligence theory, employees must demonstrate the employer had a duty to protect the information, that it breached that duty, and that the breach caused damage to the employee.

The success of these claims turns on whether employers have a legal duty to protect the information.

In a recent Pennsylvania case, Dittman v. University of Pittsburgh Medical Center, the court held that the university had no duty to protect its employees' information. Hackers obtained the names, Social Security numbers, and financial information of nearly 62,000 current and former employees. The hackers used that information to file fraudulent tax returns.

The employees argued that because they were required to provide the information as a condition of employment, the employer had a duty to protect their information. The court disagreed.

Courts consider numerous factors before imposing common law duties on employers, including:

• The relationship between the parties

• The social utility of the conduct

• The foreseeability of harm

• The consequences of imposing the duty

• The public interest in the solution

• Whether the issue has been addressed by the legislature.

In Dittman, the only factor weighing in favor of imposing a duty was the employer-employee relationship. There is obvious social utility in an employer's collection of personal information. While damage from a breach is foreseeable, the criminal act of a third party is typically considered a superseding event employers need not guard against unless they "realized, or should have realized, the likelihood of such situation."

The Dittman court reasoned that an additional duty to protect data from cyber-hacking would not further incentivize employers. Data breaches are widespread, and "there is not a safe harbor for entities storing confidential information."

Imposing a duty would require employers to incur significant security costs "where there is no true way to prevent data breaches altogether."

The significant cost increase was not justified when employers already have incentives to protect confidential information.

Courts often refuse to impose a duty on employers out of deference to legislatures. In most states, legislatures have passed statutes that define what companies must do in the event of data theft: usually notifying those affected. Those laws, however, are generally silent on the duty to protect data from disclosure. The courts reason that, if the legislature wanted to impose a duty to protect the information, it would have included that duty in the statute.

In the California case of Castillo v. Seagate Technologies, however, the court found the employer had a duty to its employees as well as their spouses and dependents whose information was compromised. Surprisingly, Seagate did not contest that it owed a duty to protect its employees' personal information.

Regardless, the court held the employees provided their information to Seagate as a condition of employment "with the understanding their employer would guard that information."

With the law on this topic in flux, employers should take reasonable steps to protect their employees' data. Any threats should be treated seriously. Data breach policies should be implemented and should account for the possibility that employee data may be stolen.

If employers discover they are victims of a data breach, they should contact counsel to develop a course of action, including assuring compliance with any breach notification laws enacted in their states.

Additional steps can also be promptly taken to mitigate damage to employees and to reduce the likelihood that they will sue.