Pennsylvania Supreme Court Lays Out Blueprint for Cybersecurity Responsibilities

PUBLISHED ON
November 30, 2018

Employees should expect their employers to store their personal information securely and out of the hands of hackers, according to a recent ruling in the Pennsylvania Supreme Court. For health care providers, this is in addition to the protections that must be used for patient data.

Employers that fail to protect their employees' information could be subject to hefty penalties similar to the ones that could be awaiting a western Pennsylvania-based health care organization.

In what could be a watershed case dictating the future of employer cybersecurity responsibility in Pennsylvania, the court ruled this week that University of Pittsburgh Medical Center is liable for a data breach that left personal information from 62,000 employees and former employees vulnerable to a data breach. It also found that the company is subject to monetary damages from a civil lawsuit brought by the affected employees.

The personal and financial information affected included names, birth dates, social security numbers, addresses, tax forms, bank account information - all information UPMC required its employees to provide as a condition of their employment. Two lower courts had previously thrown out the case, but the state's highest court revived the suit because UPMC requires employees to provide the information.

All businesses, including UPMC, must constantly assess its cybersecurity risk. This is done, in part, by understanding the vast patchwork of laws and regulations that expressly form the basis for cybersecurity liability in the instance of a data breach. Various federal, state and international laws - along with other industry-specific regulations and standards - require businesses to secure personal information.

At issue in the UPMC case was only employee information, and luckily UPMC's patient data was not compromised. Not only is UPMC now subject to the duty to protect all employee data that is required to be provided for employment, but it also must adhere to the stringent state and federal health care regulations. Health care providers are subject to extremely strict guidelines for protecting patient data and now have a duty to protect employee data as well.

The employees alleged that UPMC did not encrypt data properly, failed to establish adequate firewalls and authentication protocols. Information protected may include data owned by the business' customers, but may also include a business' own data, including personal information relating to its employees. Failure to comply with these laws and regulations can subject businesses to significant adverse consequences including sizeable sanctions imposed by governmental authorities, reputational damage and general loss of customer confidence and trust. This is true especially when its failure to comply results in an actual data breach.

An employer's duty and liability was highlighted in the UPMC case, which reminded us that these damage awards can even come from class action suits brought by the business' own employees. In its detailed and reasoned opinion, the

court held that UPMC, as an employer, has a legal duty to exercise reasonable care to safeguard its employees' sensitive personal information stored by the employer on an internet-accessible computer system. In addition, the court held that, under Pennsylvania's economic loss doctrine, recovery for monetary damages is permissible under a negligence theory provided that the plaintiff can establish the defendant's breach of a legal duty arising under common law that is independent of any duty assumed pursuant to contract.

We have learned from this case and others before it that cybersecurity and risk management begins before the data breach ever takes place and that business organizations must consider cybersecurity a legal and technological issue. This decision may expand the risk under cybersecurity insurance. Small to medium employers may need to pay more to protect their employees' data or face costly litigation if the data is hacked.

Failure to comply with vast number of cybersecurity laws or a breach of an applicable common law duty of care can trigger serious consequences. Skilled legal guidance is critical in an environment in which so many legal issues may arise, both before and after a breach. If you have any questions please contact Don Geiter, Michael Crocenzi or Elizabeth Melamed.

:

Donald R. Geiter, J.D., M.S.L. (Cybersecurity Law & Policy), CIPP/US, CIPM

Partner

Tel: (717) 399-4154

Email: dgeiter@barley.com

Michael J. Crocenzi

Partner

Tel: (717) 814-5417

Email: mcrocenzi@barley.com

Elizabeth L. Melamed

Associate

Tel: 717-399-1538

Email: emelamed@barley.com