TEXAS
EMPLOYMENT LAW LETTER
Part of your Texas Employment Law Service

September 2016

The hacker (in the office) next door

by Jacob M. Monty
Monty & Ramirez, LLP

How many employers regulate the strength of employees' passwords or have a policy against sharing passwords? To protect your business from being hacked, you may need to do both.

Don't pass it on

We typically think of hackers as computer geniuses who create sophisticated codes and infiltrate complex technology systems. But in today's world, simply knowing someone else's password can do the trick. Former St. Louis Cardinals executive Christopher Correa is in prison for accessing the Houston Astros' scouting databases. He was no computer genius; he simply knew an Astros employee's password.

Sensitive information is constantly at our fingertips, and it tends to travel with us. Laptops, tablets, and cell phones should all be password-protected, and employees should use strong passwords that contain letters, numbers, and special characters. And, for heaven's sake, they should never tuck a list of their passwords in their computer cases.

Instruct your employees to create completely new passwords for work purposes. An employee's password shouldn't be similar to the password she used for a former employer, and it shouldn't be the same password she and her spouse use to access their personal bank account. Competing former employees or angry spouses should never have the ability to access your company's confidential information. You should also work with IT to create appropriate firewalls and safeguards, including the ability to wipe an employee's company-provided cell phone if it's lost or stolen.

It's also important to prohibit employees from sharing their passwords. Password-sharing could create personnel and morale issues. For example, an employee with access to her supervisor's e-mail might find out that her coworker is being terminated.

Serious legal issues could also arise when employees share devices or passwords. For example, a manager with a dead cell phone battery who borrows a subordinate's phone for work-related purposes might see a text message about the employee's union activity flash across the screen. The next time the manager disciplines him for misconduct at work, the employee could claim that the discipline was retaliation based on his protected concerted activity. And the National Labor Relations Board (NLRB) could determine that the manager engaged in unlawful surveillance.

Prying eyes can lead to liability

An employee may also use a coworker's password to view information he shouldn't have access to, such as personnel files to support a potential lawsuit or payroll files to satisfy his curiosity about other employees' wages. That can create significant liability for Texas companies.

Under Texas law, companies have a business duty to protect employees' sensitive personal information, and you are required to notify workers if someone gains unauthorized access to computerized data that contains their sensitive personal information. "Sensitive personal information" is defined to include an individual's first and last name in combination with their social security number or driver's license number. Civil penalties of $100 per individual, up to $250,000, apply for every day an employer fails to take reasonable action to comply with the notification requirement.

Texas businesses are required to implement and maintain reasonable procedures to protect sensitive personal information from unlawful use or disclosure, including taking any appropriate corrective action. Additionally, courts tend to uphold negligence or breach of fiduciary duty claims in data breach cases. There's also potential liability for common-law invasion of privacy.

In addition to federal laws that prohibit hacking, Texas has a "breach of computer security" statute that prohibits knowingly accessing a computer or computer system without the owner's effective consent. "Computer" is defined generally to include devices such as cell phones. A guilty individual can be punished by a fine up to $2,000, jail up to 180 days, or both; a guilty corporation can face a fine up to $10,000.

Bottom line

Protect your confidential information, and protect your business. Instruct your employees to create strong passwords and keep them private. Use IT services to ensure that your data is as safe as possible. If you find out that someone had unauthorized access to sensitive information, take corrective action, and ensure you've

complied with all notification requirements under Texas law. Today's hacker might simply be the employee in the office next door who happened to see your four-digit phone passcode.

Jacob M. Monty is the managing partner of Monty & Ramirez, LLP and an editor of Texas Employment Law Letter. He can be reached at jmonty@montyramirezlaw.com.