A Former Employee Stole Our Computer Data - What Do We Do First?

by Stephen E. Yoch - Monday, April 17, 2017

It is an all too common experience when an employee announces he or she is leaving and shortly thereafter huge amounts of a company's data are missing, sabotaged, or evidence shows massive downloads by the employee on the eve of their exodus.

The natural tendency of a victim to such an attack is to dig through the employee's computer to ascertain what occurred, or take the former employee's computer and put it to productive use with another employee. In other words, make the best of a bad situation. Unfortunately, this natural instinct is the worst thing a company can do. Digging through the former employee's computer or re-tasking the computer may permanently inhibit the company's ability to pursue a criminal claim or file a civil claim seeking damages caused by the former employee's actions.

The Critical First Step

Taking or destroying computer data is a form of conversion (a lawyerly word for theft). As with any crime, it is important to preserve the evidence. Everyone understands from watching television the importance of making sure evidence of a crime is preserved for trial. The same is true if electronic data has been disrupted or taken. If a company is a victim of the destruction or taking of data, its first step needs to be preserving the crime scene – in this case segregating the exiting employee's computer.

A complete forensic copy of the employee's computer needs to be made immediately following the employee's exodus. A forensic copy permits experts to examine exactly what occurred in the computer and potentially provide information which could be used in a civil and/or criminal prosecution against the wrongdoing former employee. The continuing use of the computer after

the employee leaves or allowing the company's IT department to examine the computer can irreparably damage the forensic evidence of wrongdoing, just like disrupting a crime scene.

The good news is once a forensic copy is made, the offending computer can be re-used productively by other employees, and the forensic copy can be carefully examined without fear of disrupting the record or damaging data.

Bottom Line

Put simply, if you think your former employee engaged in improper destruction or taking of computer data, your first step needs to be obtaining a forensic copy of the former employee's computer. To do otherwise may render any possible future claim impossible.

---

220 South 6th St, Suite 2200, Minneapolis, Minnesota 55402 612-339-6321 | 800-989-6321