

2/16/2009

Now What? Calm Urged When Theft Hits Your Company

By Adam D.H. Grant

The president of a company comes to work one morning and listens to his phone messages. One ominous message is from a district attorney about his chief financial officer. Intrigued, he returns the call. The district attorney says that the financial officer, who has been employed by the company for two years and has not yet returned from a vacation, has been arrested and accused of embezzling from his prior employer. Concerned about his company's own finances, the president calls his accountant. It appears that the company has been attempting to collect on past due accounts, but customers are claiming payments have been made. The company books do not reflect these payments. There is a problem. What would you do?

It's time to stay calm and make decisions that could affect the severity of the loss and the future health of your business. Here's a step-by-step action plan to find the perpetrator, preserve assets, reduce negative publicity, maintain employee morale, prevent further loss and explore insurance and legal options when a breach occurs.

Information Preservation

In the throes of a crisis, quick action is necessary. Where is the company's most sensitive information? Where are bank statements and loan documents? Identify and locate information that is the most likely to be affected by the breach. For example—offsite copies of bank statements are a low priority; an onsite checkbook could be a high priority.

Regardless of what was stolen—money, products or intellectual property—immediately backup all company data on servers, stand-alone PCs and PDAs. Stop automatic purging of files, e-mails and other data. Strategize with IT personnel to determine any additional ways to safeguard confidential data.

If you later find that information has been altered or erased on an electronic device, a forensic information technology expert can evaluate the electronic fingerprints left behind—who accessed data last and what was changed. Even so, preserving data immediately prevents an electronic "paper trail" from being destroyed.

Consider, as a matter of company policy, to image hard copy documents and store the files offsite. When a crisis hits and hard copy documents are mysteriously missing, the backup could be invaluable in determining the severity of the loss and possibly point to the culprit.

Identify who has access to confidential information. Every business should maintain a list of who has passwords for sensitive information sources—computers, online banking, ATM machines, security systems, safety deposit boxes and investment accounts. While trusted employees are given these passwords, without proper password security, they can easily fall into the wrong hands.

Bottom line: every business should have a data preservation policy in place to protect sensitive information. This policy will not only prevent breaches from occurring, but will make tracking down the guilty party that much easier.

Responding to the Media

Depending on the severity of the breach, the loss may attract media attention. In these cases, the company should first determine the message it wants to present to the public and develop a plan to disseminate the message through the media.

The company spokesperson (ideally the company president or CEO) must be well versed in media communications. The spokesperson (and there should be only one) must stay on message in media interviews and through written communication. The message needs to be an honest account of the theft (staying within the guidelines of any criminal investigation) and present a proactive response of how the company is responding to the loss.

Never hide behind "no comment" or fail to return media telephone calls. These actions allow others to determine the company message—whether accurate or not.

Employee Relations - How to Prevent Rumors and Shore Up Morale

Employees need to be informed about the breach especially if the loss came from within. Most often, information to employees is delivered through human resources, but if the breach is severe, the company president or other high level executive may be selected to keep employees initially informed.

By dispensing forthright information quickly to employees, the company reduces rumors. The worst move for management is to go behind closed doors for several days while employees hear nothing. Management needs to communicate quickly to employees; otherwise, the rumor mill will create a situation that is far worse than reality. Morale suffers in an information vacuum. By sharing what you know, you create a closer bond with employees who are then more willing to contribute information that could help with the loss investigation.

Cast of Characters

If your inquiry leads you to suspect a specific employee, look at his or her coworkers, vendors and others who could be involved. When the breach is a crime of opportunity (the perpetrator sees the opportunity for quick cash or to steal goods), usually only one person is the culprit. If the crime is more calculated, the theft usually involves two or more people.

Recovering What's Been Lost

If the loss is significant or has taken place over a long period, there is hope that assets can be recovered through an asset check.



In one case, an asset check was conducted on a company CFO. He had embezzled \$2.4 million and the investigation found he had invested the money in six pieces of property. He was sued and a lien was placed on the properties. Eventually, the case was settled and the company took possession of the properties and sold them for a gain. The CFO? He spent 4 ½ years in prison. In most cases when a police report is filed, an “order of restitution” is obtained and executed much like a settlement.

Insurance Coverage

“Employee dishonesty” insurance covers company theft. Some coverage limits are as low as \$50,000; others are in the millions. How do you determine the coverage limit best for your company? It depends on company size and type. A large manufacturer, for example, may receive sizable payments from customers, so a \$500,000 or \$1 million policy limit may be appropriate. For a small mom and pop retail outlet, a \$50,000 policy limit would probably be sufficient. Most theft amounts are under \$50,000. The crime is committed by people who need quick cash—maybe for a nefarious drug habit, a medical emergency or to pay bills

Adam D.H. Grant is a principal with the Encino law firm of Alpert, Barr & Grant, APLC and is a Trustee for the San Fernando Valley Bar Association. His practice areas include complex business litigation, construction law, real estate and general liability claims. He can be reached at agrant@alpertbarr.com