Physical Controls in an Internal Control World

In the fraud prevention game, we often hear the term "internal controls" thrown around. This term refers to using a control system within a company to prevent the theft of sensitive or classified information, inventory or money. Much like the term implies, physical controls are more likely seen or touched than the internal control system. It is one thing to implement an internal control system, but without physical controls the internal controls are pretty useless. Face it, we do not just put inmates in a prison and let them hang out until their sentence is completed. No, we put them in a prison, behind bars, walls, doors, fences and gates and only let them out at certain times of the day in a controlled environment so that the guards can maintain control of the group that vastly outnumbers them. The same principals apply to your business.

Think of physical controls as your overall security system. For example, the door to your office building probably has a lock. Who has access to the building outside of business hours? Do all employees have a key or access code? Do you know who is on the premises and when? Who opens and closes the building each day? The building may also have a security system. Do all users share the same passcode and security level? In a small business, all but the owner or manager probably have a similar access setup. In a larger company, it is probably easier to set parameters, but possibly harder to monitor access to the overall building.

Once in the building, is your business an open layout where everyone has access to everything or are individual offices and desks locked up? Are sensitive documents and money stored in a secured area? What about inventory? If someone were want to, could they walk right out the front door with company assets? This is important for many reasons. A client's sensitive personal information could walk out and make its way to the black market or be used mischievously. A company could be losing hundreds of thousands of dollars each year with inventory walking out the door. Private personnel files could be gone through and leveraged against the management, or other employees of the company. Again, granting access to employees or visitors without some sort of physical control is going to harm the business at some point.

The easiest way to prevent theft is obviously to lock up sensitive items, money or inventory. The lock itself is a deterrent. To get past the lock, one is going to have to do some work to either "pick" it, or to steal a key or swindle access to it. Most people do not want to work that hard. Next, based on job description determine who needs access to what. An employee in one division of the company does not necessarily need ready access to information from another division of the company. Only grant access to those that need it, when they need it. Although we live in a 24/7/365 world it doesn't mean that employees need access under those terms. If employees do not need to be in the building after hours or on weekends, they should not have the ability to do so. By simply restricting access a company can send a message to any potential fraudster that they are going to have to work around the system and increase their chances of getting caught should they choose to commit a fraud.

In addition to filing cabinets, offices, desks, the building, files, inventory, etc. an easy way to prevent theft is to lock your computer when away from it. Simply press the "CTRL", "ALT" and "DELETE" buttons in unison and select "lock". This will keep other employees off of your

computer while you are away unless you have shared your password with them. It is never recommended to share passwords for computers, email or the security system. A user ID and password are identifiers employers can use to help identify who may have committed a fraud or theft. Also, not every employee may need access to every type of program. An employee in sales probably doesn't need access to the company's payroll or payables files. Only grant access to those that need it.

Many businesses have chosen to implement additional security measures. With the cost and availability of video security systems reaching an affordable peak the implementation of those has increased to the point that there is no privacy anywhere any longer. Like they say, a picture is worth a thousand words. If something shows up on video, it makes it that much easier to prosecute. Some businesses still employ security inspections at ingress and egress throughout the building whether through physical measures or through access card measures. The sheer fact that someone may be watching is a strong deterrent for a potential fraudster.

Speaking of watching people, it is important to conduct periodic, unannounced examinations of inventory, checks, cash, files, etc. If an unethical employee knows that an examination is coming this gives them time to conceal their fraud by altering or destroying evidence that may point to them being a guilty party. This is not something that should be done only on an annual basis during audit time.

If physical controls are going to be taken seriously by the employees, they must be taken seriously by management and ownership. The tone at the top is important and will place everyone on notice that physical controls are taken seriously. Policies must be set and in place prior to any unethical behavior taking place. If there is a punishment for unethical behavior, it must be implemented quickly and consistently across the board. There should not be one set of rules for one group, and another set of rules for another group. All groups need to be on equal ground when it comes to punishment and expectations. Everyone should know how to report unethical behavior within the company. Whether that process is through management or a separate whistleblower hotline. Make sure the process is posted where everyone can see it. It is also important to ensure all employees are trained on physical controls company wide. This way, there is no excuse that someone did not know they were accessing a restricted area or viewing restricted information.

The loss to a business for not implementing physical controls can be disastrous. Every effort should be made to address any issue immediately so as to minimize the loss. Implementing, and actually following, a strict physical control process in tandem with an internal control process can ensure that everyone from ownership, management, employees and customers can feel safe and secure that all information, products, funds, etc. are safe is of the utmost importance to any business.