Steps to Prevent Corporate Espionage

The following sections outline some steps that help in preventing corporate espionage.

Understand and Prioritize Critical Assets

An administrator needs to determine the criteria that are used to estimate value. Monetary worth, future benefit to the company, and competitive advantage are sample criteria that could be used. Whatever the criteria are, they need to be determined first.

After all assets are scored, the administrator needs to prioritize them based on the criteria. When the administrator is done, he or she should have a list of all the critical assets across the organization. These assets represent the crown jewels of the organization and need to be properly protected. Once the list of assets has been determined, the critical assets need to be protected. An administrator needs to understand the likely attack points and how an attacker would compromise each asset.

Define Acceptable Level of Loss

The possibility for loss is all around, and risk management becomes a driving factor in determining what an organization should focus its efforts on and what can be ignored. As difficult as it may seem for all critical assets, an adequate level of risk needs to be defined. This helps an organization to focus on what should or should not be done with regard to insider threats. Cost-benefit analysis is a typical method of determining the acceptable level of risk. The general premise behind cost-benefit analysis is determining what the cost is if the asset is lost in part or in whole, versus what the cost is to prevent that loss. While this is hard for some people to swallow, there are actually many situations where it is more cost effective to do nothing about the risk than to try to prevent or reduce the risk from occurring.

Typically, there are two methods to deal with potential loss: prevention and detection. Preventive measures are more expensive than detective measures. With a preventive measure, the organization stops the risk from occurring. With detective measures, the organization allows the loss to occur but detects it in a timely manner to reduce the time period in which the loss occurs. Defining an acceptable level of loss enables an organization to determine whether it should implement preventive or detective measures. If the organization's acceptable level of loss is low, which means it has a low tolerance for a loss of a given asset, a preventive measure would be more appropriate to stop the loss. The organization would have to be willing to spend the extra money on appropriate preventive measures. If the organization's acceptable level of loss is high, this means it has a higher tolerance and would most likely spend less money on a solution and implement detective measures. Now, the organization is allowing the loss to occur, but it is controlling and bounding it. Therefore, performing calculations on acceptable level of loss plays a critical role in controlling insider threats.

Control Access

The best method for controlling insider threats is limiting and controlling access. In almost every situation in which an insider compromises, it is usually because someone had more access than he or she needed to do his or her job. There are usually other factors at play, but the number one factor is properly controlling access. For preventing insider attack, it is better to allocate someone the least amount of access that he or she needs to do his or her job. Encrypt the most critical data. Never store sensitive information on a networked computer; store confidential data on a standalone computer that has no connection to other computers and the telephone line. Regularly change the password of confidential files.

Bait: Honeypots and Honeytokens

A honeypot is a system that is put on a network that has no legitimate function. It is set up to look attractive to attackers and keep them out of critical network systems. The key thing about a honeypot is that there is no legitimate use for it, so no one should be accessing it. If someone accesses the honeypot in any way, that person is automatically suspicious because the only way he or she could have found it is if he or she was wandering around