HOW ARE YOU MITIGATING THE MALICIOUS INSIDER THREAT?

The news often focuses on cyber breaches, ransomware and other external threats.

What we don't see or hear about as often is the risk of insider threats which are just as serious in terms of the potential damage.

Insider threats are often harder to find and then determine if the action was indeed a malicious action, an innocent action, or a simple error. What makes them hard to detect is that insiders need access to confidential information to do their jobs.

This access can be exploited by an outside party who convinces an employee to send confidential data. They may have offered money for the data or used ideology to convince the employee to send the data.

The other possibility is simply an error either in the actions of the employee or in the interpretation of the action. For instance, an employee is found accessing files they don't normally need. This can be innocent if the employee needed the information for something specific or maybe accessed a file in error.

In another situation an employee downloaded a number of files to a memory stick or their laptop. Certainly, this should raise red flags. But what if they are going on a cruise or a flight or to a place with limited network access and want to be able to work on the files?

What this shows is that insider threats are not as clear cut as discovering an external party in the systems. These situations require interpretation and often speaking with the suspected party. That is why the one who reviews possible insider threats needs to have excellent interpersonal skills in addition to good cyber skills. This team or person needs specialized training in how to detect when someone is lying.

This specialized team should be the first one to review suspicious activities and not the HR or Legal teams.

This team needs a good working relationship with HR and Legal as they may need to be brought in.

There are actions you can take to minimize insider threats. First is to create the team mentioned above and provide the necessary training.

Set up your systems to log users and files being accessed, downloaded or transferred. Many cloud platforms have the capability to do this. These logs can be used to send alerts of suspicious activity to the team. The logs can also serve as evidence if necessary.

Being proactive in learning the risks and the appropriate course of action is an excellent beginning in protecting against insider threats.

Want to learn more about cyber security and education, contact AIM Cyber at info@AIMglb.com or call (888) 773-1920.