HOW TO MAKE A RANSOMWARE ATTACK WORSE

Your company just become the victim of a successful ransomware attack. Things can't get any worse. Or can they?

Yes, how you respond has a major impact on whether things get better or worse, and whether your company survives or not.

Responding well takes preparation and training. Don't think you can work it out after the ransomware attack, you can't.

First and most important is an incident response plan that addresses all affected areas including IT, customers, regulators, employees, law enforcement and the media. It needs to be detailed enough to cover everything and be clear about responsibilities.

This is especially true for communicating with the media. Reporters will call everyone they can to get information. And nothing is ever "off the record."

The IT group's first response is often an attempt to reclaim the data. But this is an error. The first action should be to prevent the ransomware from spreading. Be sure you have an accurate up to date backup that is safe from the ransomware. If it is on the network the ransomware will find and encrypt it rendering it useless. Don't forget the backup needs to be available. Document where the backup is located and how to access and implement it.

Do not waste time looking for decryption keys. The key may be available on the internet but the odds of that and of it working are slim. Wasting too much time searching for the key can give the infection time to spread or for the attackers to raise the amount of ransom demanded.

Ask for help, ransomware attacks are events that can destroy your business. You would not face a lawsuit without contacting your attorneys. Be sure to contact them for this also and engage law enforcement. They are knowledgeable about ransomware and how to respond to it.

Contact your insurance company sooner rather than later. Waiting too long may mean failing to take certain actions they require for coverage. If that happens the company can deny payment.

Be sure to engage advisors who are familiar with ransomware and the current environment and specifics for the different ransomware gangs. Ransomware attackers often put other forms of malware on your systems. Engage a firm that specializes in finding and removing malware.

After the event when things are back to normal, conduct a review and use what has been learned to help prevent a repeat.

Remember, without proper training for all employees at every level, the incident response plan is just a waste of paper.

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