BEING BREACHED IS ONLY PART OF THE PROBLEM

Too often when a breach occurs the company may not even find out about it for days, weeks, or even months. Then what happens? Little communication or perhaps denial thinking if they don't admit it, the bad publicity will go away.

But it doesn't. In fact, failing to communicate openly and honestly is just asking for trouble.

Breaches are expensive in downtime, legal fees, restoring the systems, reporting to regulators. And if ransomware, the ransom.

The highest cost can be none of these but the reputational damage. This will be highest in industries where trust is an essential part of the relationship. Yes, in any industry if I give my name, email and a credit card number I expect it to be properly protected. Not just glossed over.

For healthcare, banking, investments, law, real estate and other service sectors trust is as important as professional expertise. After all, you are giving them very private information that is on the cyber criminals list of most wanted information. The cyber criminals want it to cause damage or to sell to others who will use it to cause damage.

When you are breached, people will look at how their private information was protected and how you communicate. People are used to seeing breaches in the news but think of the damage if you don't communicate openly and people feel you are deceptive. Or worse yet, it comes to light that you were hiding that you didn't properly protect the data. The penalties will be substantial, the recovery costs will be substantial, but will you survive the loss of trust?

A Communication plan is the answer to this. Not just creating it, but using it. Be sure to assign communications to senior people who understand the value of communication and how to communicate. Everyone needs to know who is in charge and who to direct media inquiries to. Because the media will call everyone they can looking for information. One mis-step by an employee who thinks they are doing good, or doesn't understand the importance of communication, or really believes what they say is off the record, and your reputation can be trash.

Once the breach occurs it is too late. Begin to prepare now. Learn what needs to be done to protect the private information entrusted to you. Learn if your technology environment is properly protected. Learn how to educate people on what to do and not do to protect data.

And equally importantly, create an incident response plan and a communication plan to keep all interested parties informed.

Learn all that needs to be done and then do it.

Now is the time.

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