TOOLS ALONE ARE NOT THE ANSWER

Everyone has at least one cyber protection tool on their computer. Yet, we hear about new breaches every week. Clearly, if tools alone prevented cyber breaches, there wouldn't be any more.

Tools are a necessary part of cyber protection but only one part of a comprehensive holistic cyber protection plan.

Interestingly, a cybercriminal that encrypted a company's files sent a message along with the instructions on how to decrypt their files after the ransom was paid. The message said to use more than just simple antivirus tools and use 2 factor authentication, to backup files regularly to something not on your network, or it will also fall victim to the ransomware.

These are good suggestions. But alone will not prevent breaches. So, what is causing the successful breaches? Research shows that people are the weak link in the cyber protection chain with 95% of the breaches caused by human error.

The best way to prevent human error is by training and ongoing testing. Training needs to be formal and organized. Regulators and cyber insurers want to see training records of who was trained, the content of the training, when the training took place, and the results of an exam demonstrating understanding. If this cannot be shown, regulators can impose fines and cyber insurers can refuse to pay the claim. This should convince you of the importance of training.

Cybersecurity training needs to begin at the top. If company management considers training as just a "box to check" then that is how employees will see it. And the results will show.

The ongoing testing needs to be conducted in a way that people cannot tell it is a test. This will show who falls for the phishing emails and needs more training.

If training and tools are essential parts of cyber protection what else is needed?

To do it properly, cybersecurity has to be looked at holistically - as a continuous cycle beginning with a strategy for any family or organization attempting to create better cyber protection and response capabilities.

Cyber risks are not going away anytime soon. In fact, cybercriminals are getting more devious all the time. Protecting information is crucial whether it is your family or your business. And a business must also protect the information of their clients, customers, or patients.

Cybersecurity is not a one-time event. It is ongoing because cybercriminals are relentless in their attacks and the schemes devised to steal information.

Be just as relentless in protecting your information.

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