AIM CYBER

High-touch services to help you navigate modern cyber threats.

MAKE SURE SECURITY KEEPS PACE WITH IT

We’ve written before about how the recent COVID-19 pandemic pushed the move to the cloud and support for many more remote workers. And much of it was good. Allowing people to work remotely kept businesses open and people safe. A good combination.

The two trends are related in that the move to the cloud facilitated the work from home, WFH, boom. WFH allowed companies to benefit from the flexibility offered by the cloud. And the flexibility of the cloud made it easier to support the WFH numbers.

Certainly, the move to the cloud was already in progress before the COVID-19 pandemic hit. But it happened significantly faster.

WFH was happening as more companies realized the savings in real estate and other costs it offered. No one expected WFH to be almost all employees. But that happened quickly and allowed business to function. With the pandemic coming more under control through the vaccine, research shows that most companies forecast 25-30% of employees will be working from home at least a few days a week going forward.

As with anything done too quickly, the rapid shift also had its downsides. In this case the big one was, and still is, security. Moving your entire IT shop to the cloud while working to support an increase in remote workers is challenging to say the least.

And on the whole IT teams faced the impossible and accomplished it. Not everything was migrated to the cloud but that is a good thing. Some applications work better in a local environment giving a hybrid cloud model which is a new architectural model to many IT teams. With a new architecture comes new challenges. Usually the model would be vetted and rolled out slowly giving time to troubleshoot and fine tune it. But here it was almost instantaneous with little or no time to test or adjust. Security was sacrificed for speed to keep the company operating.

Now is the time to revisit everything and look at security. Many companies didn’t or still don't understand that cloud providers secure only their infrastructure, nothing more. Each cloud customer is responsible for securing their applications and the data in each.

A number of breaches from improperly secured databases, applications or cloud environments. made the news.

The hybrid model fits the needs of many companies and applications but also complicates security with two separate environments and architectures to secure. Remember attackers attack. They don’t differentiate between in-house and cloud environments. They want your data or to encrypt it with ransomware regardless of where it lives.

The rush to the cloud is over for most companies. If you haven’t already, revisit the architectures and all settings to make sure everything is properly protected. Don't forget to check that all default passwords have been changed. Ignore or postpone security at your own risk. You may have made it through the pandemic, but will you make it through a breach, especially if the news reports your protections were inadequate or negligent.

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