HYBRID MODELS AND RANSOMWARE - A MARRIAGE MADE IN XXXX

When the impact of the pandemic became widespread, businesses closed the offices and sent employees to work from home. This was the right thing to do to keep people safe.

But it created big cyber risks as employees moved from office systems with many protections to home computers, home routers and home WiFi networks with far less protections.

Cybercriminals saw the change and did their best to exploit it. Sadly, they were rather successful as evidenced by the dramatic rise of successful ransomware attacks; a 41% increase in attacks in 2021 alone, and a 93% increase compared to 2020.
And the ransoms also increased. The recent CNA attack has the unofficial record at $40 million.

Getting started in the ransomware business has never been easier. Ransomware as a Service, RaaS, is a real thing. Developers of ransomware offer it to anyone willing to pay. And sometimes it is done as a percentage of the ransom collected so there is little to no upfront cost for someone wanting to start a ransomware business.

But now the pandemic is winding down in this country and others, and businesses are beginning to reopen.

The new model for many companies is a hybrid with employees spending some days in the office and some days working at home.

Ransomware attackers have relied on humans clicking bad links to download the ransomware. Reports say 90-95% of the successful attacks are caused by human error. That means falling for phishing and other scams.

The past year showed taught us that people are more likely to click a bad link at home than at the office. All this means ransomware will continue to grow.

For companies, the new hybrid model may come with a high degree of unexpected risk.

Making matters worse, attackers are expanding their methods by working with cybercriminals who have already penetrated a company network and sell that access. This new attack method can take advantage of any weakness in the defenses such as those found using home computers, routers and wifi networks.

Ransomware attacks are costly. Even if companies have encrypted backups, it takes time to restore everything. And during that time the company may not be able to function. Small companies may not survive.

What to do? As the old saying goes, the best defense is a good offense. In this case it is educating users, so they know what to look for and where not to click.

It may not be 100% successful but since ransomware, for the vast majority still relies on people clicking bad links, education will certainly help.

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