BLOG

Cybersecurity and Cloud Solutions

By Zach Altneu, Cyber Insurance Broker

Apr 2, 2021

The COVID-19 pandemic has led to an acceleration of adoption of cloud solutions and other remote access tools, with many businesses choosing to put aside previous concerns about potential security risks to accommodate a remote workforce. However, hasty adoption of any new technology that is not combined with robust security frameworks, policies and controls can leave businesses vulnerable. A formal vendor management process and having specific controls in place can mean the difference between a cloud solution being a huge advantage to agile operations or leaving the business open to attacks and unauthorized access.

Cloud Technology

Cloud computing solutions give companies greater flexibility, help to reduce costs, and improve security – just a few of the reasons why companies are migrating at least part of their operations away from traditional servers. Even if you are working primarily on a physical server connected to the network, you can still utilize cloud solutions to back up your data on a remote server. Backing up data on a cloud server separates the data from the core network and servers, providing an extra layer of protection if a bad actor were to access the network. The logic being that with the right password and credential management policies, even if that bad actor makes their way onto the network with stolen credentials, hopefully the credentials for the cloud solution are different than those of the network, stopping them in their tracks. Most cloud providers also have the ability to easily set up multifactor authentication as an additional layer of security, which we recommend taking advantage of whenever possible.

As decentralized systems, cloud backups and servers are not on network devices, which can make it more difficult for someone outside of the company to gain access over them and potentially your data. Some believe that the cloud must be inherently less secure because it is accessible through the internet, but it is precisely that remoteness and disconnect from the core network, in tandem with the additional correct controls, that can protect your company.

Vendors

Some larger businesses are able to set up their own data centers and manage private cloud servers for themselves, but they are in the minority. Most will turn to what is known as the “public cloud” and large vendors to set up servers for their company. There is always inherent risk in that relationship, as there is

with giving data and network access to any vendor that you choose to do business with.

As we constantly tell our clients: vendor due diligence is critical, no matter what service or solution you're seeking. Make sure you are doing your research with your cloud provider. Here are some common questions to ask:

- Are they using the right security solutions, and do they have the right security controls in place?
- Where will the data be stored?
- What systems are being used and are they up to date?
- Is my company's data separated from other entities'? What are the access and security permissions/controls?
- Are they using encryption?

You are entrusting this provider with your company's data and if there is an incident on their systems, **you** will be held responsible for the liability that could arise, not them. So, whether they're one of the behemoths that dominate the space – Amazon Web Services (AWS), Microsoft Azure, Google Cloud – or a lesser known enterprise, make sure you have done your homework. In addition, many of the providers have contracts with each other. VMware, for example, has a partnership with AWS which means that while your contract might be with VMware, your data is likely being hosted on an Amazon cloud server. It is important to know exactly where your data is being stored as you are responsible for it.

Cybersecurity Policies

Regardless of how reputable your cloud provider may be, a strong cybersecurity policy is absolutely imperative and should be updated to reflect any new cloud-based tech that you've implemented.

Due to the rampant increased severity and frequency of ransomware attacks, the cyber insurance market is rapidly evolving and hardening. Underwriters are being more discerning when it comes to specific security controls and there is a real emphasis on putting in place measures like multifactor authentication. MFA specifically has become almost a pre-requisite for obtaining coverage with many carriers. They are also asking more questions – for instance, they will ask if you're using cloud backups, what provider you're utilizing, if they are using encryption and so on. Carriers are looking particularly fondly on businesses that have offsite backups for their files and servers. Larger companies may set up their own private data centers for this purpose, but for smaller to medium sized enterprises, this is exactly why cloud computing exists: a cost-effective and fast way to set up, backup, protect and restore data and servers without incurring the costs associated with setting up and maintaining a data center offsite.

Going forward, we expect many businesses to remain open to housing an increasingly remote workforce on a permanent basis, which certainly means that cloud computing in many forms is here to stay. With a strong cybersecurity policy and the right controls in place, businesses should feel confident about embracing cloud solutions, and insurers will look more positively on their risk profile as well.

Want to learn more?

Find me on LinkedIn, here.

Connect with the Risk Strategies Cyber Risk team at cyber@risk-strategies.com.

Email me directly at zaltneu@risk-strategies.com.

TAGS:
Cyber Liability