Backups are the Key to Cyber-defense

Posted At : August 28, 2020 9:32 AM | Posted By : Admin
Related Categories: Your Business, Security

It has been common for most businesses, organizations, and individuals to invest in preventative cybersecurity defenses. Most organizations have technologies such as firewalls and anti-virus software that are designed to stop a cyber-attack. These controls certainly serve a purpose in fighting the war against cybercrime and should not be discounted.

But, cybersecurity professionals are recommending that we turn our attention to our ability to detect cybersecurity incidents and recover from them.

It makes perfect sense. The reality is that defending against all cyber-attacks is an incredibly hard task to do. Hackers are anonymous, perimeters are not physical, attacks are sophisticated, and the volume of cyber assaults launched every day is astounding. Defending against all cyber-attacks is a little like entering a cage fight blindfolded with one arm tied behind your back. Despite the best defensive efforts, you will get hit.

Hence the recommendation to invest the ability to recover from a cybersecurity incident. Of course we will continue to defend ourselves from cyber criminals, but we also recognize we are not fighting a fair fight, and that we may likely suffer a cyber incident at some point. The thought is simple: If or when we become a victim of cybercrime, we must be prepared to recover from the incident. We can then weather the storm.

BACKUPS ARE KEY

If you do not regularly backup critical data and systems, then you must start doing so immediately. If you do not have a documented disaster recovery plan, then you must create one immediately. In the process of creating a data backup strategy and disaster recovery plan, please recognize the nine most common mistakes made and more importantly, how you can avoid making them in your quest for recovery preparation.

While most companies have backup systems, we find that there are important aspects missing in how backups are setup and integrated into a cyber-defense program. Here are the common issues we see out there:

1. **The Scope of the Backup is Incomplete.** It is very common to see a data backup that has very little strategic thought behind it. Evidence of this mistake presents itself in the form of:

- Important Data, Applications, or Systems that are NOT included in the backup job(s).
- All Data, Applications and Systems are backed up the exact same way – there are no priorities.
- The time it takes to ACTUALLY recover lost or corrupt data is much longer than expected.
- The point in time in which you are ACTUALLY able to restore to is too far in the past (I want to recover yesterday's information, but I am only able to recover last month's information!)

Avoid this mistake by classifying and prioritizing the data, applications and systems that need to be backed up. A Business Impact Analysis will identify critical sets of data and define Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO). This allows you to implement a backup job that supports lightning fast restore times for critical information.

2. **Backups are Not Completed Automatically.** All too often we see backup jobs that require a person to manually start the backup. The process to start the backup job is usually very simple, like clicking a button. However – PEOPLE FORGET TO DO IT!! Backup jobs should always be automated. Automation eliminates human error or neglect and yields a much better chance of having a successful backup when you need it most.

3. **There is Only ONE Copy of the Backup.** There should always be more than one copy of your data backup. For critical systems, we recommend having three copies – for less critical systems, we recommend having two copies. The logic is simple, what happens if your data backup is lost, deleted or becomes corrupt? If you need to restore from backup, is it more comforting to have only one recovery source, or is it more comforting to have a few recovery sources?

4. **Backups are Not Monitored for Success.** So many businesses have a "set it and forget it" mentality about their data backup jobs. NO ONE EVER CHECKS TO SEE IF THE BACKUPS ARE SUCCESSFUL!! For this reason it is important that your backup jobs are monitored very closely and if there are any errors (and there will be from time to time) that cause a backup job to fail – YOU NEED TO BE NOTIFIED. There are many systems that are available to provide monitoring and alerting services for backup jobs. You must keep a close eye on your backups; otherwise you will find yourself in a very bad situation one day.

5. **Backups are Not Kept Offsite.** It is very common for data backups to be kept onsite, in the same physical location of

the systems that are being backed up. While this practice is acceptable for some types of system failures (hardware failure, software corruption, etc.), it is a terrible idea for other types of failures. For example, if your building floods or burns – and your servers are severely damaged – do you think the backup media that was located right next to those servers will also be damaged? YES, IT WILL BE! For this reason, it is important to keep at least one copy of your data backups offsite, at a different physical location.

6. **There is Insufficient Capacity for Backups.** The backup job is 400GB, but your backup tape or drive is only 300GB. Capacity issues have a tendency to create sloppy and incomplete backup jobs. It is imperative that your backup media be sized and provisioned to not only support your current backup needs, but also allow for some element of growth over time. A simple Capacity Planning exercise conducted by a qualified technician is incredibly important to your overall backup strategy.

7. **There is No Documented Disaster Recovery Plan.** Often we see backup jobs that are working very well. Critical data is being backed up at regular intervals which support organizational RTO and RPO requirements. Then, disaster strikes. There is a power outage that fries the server, the network room floods, the building burns down, etc. A backup job is only successful if data can be easily and quickly recovered. You need to have a recovery procedure documented! Typically this is in the form of a Disaster Recovery (DR) Plan. The plan should include important procedural steps involved in recovering lost data and should also indicate who is responsible for performing those steps once a disaster is declared. If you choose to not have a documented DR Plan then recovering from a disaster will be chaotic and frustrating at best!

8. **There is No Process to Add or Remove Items from the Backup Scope.** As new servers, applications and data repositories are added to your computing environment – they also need to be added to your backup job(s). It is very important to have a documented Data Backup Policy that outlines the process for adding or deleting components of the data backup job(s). Without a policy, new systems may or may not be integrated into the backup job(s) effectively and old systems may never get removed. Once you have a great data backup job, you want it to stay great. This requires governance and oversight typically provided by good policies and procedures.

9. **Backups are Not Tested; People are Not Trained.** Data backup job(s) absolutely, positively need to be tested AT LEAST ONCE A YEAR at an absolute minimum - QUARTERLY is far better. A true test is the only way to verify that critical information can be restored if needed. More importantly, people (employees, vendors, etc.) should all be educated on the restore process, especially if they play a critical role in restoring lost or corrupted data. A common and effective way to provide this training is by conducting routine Table Top exercises where DR scenarios are presented to the recovery team and they have an opportunity to respond – without creating any service disruptions

The Computing Center provides consulting, products, services, and the knowhow to help you setup and manage backup and disaster recovery systems. We partner with many of the most innovative providors in IT to get our clients the most cost effective systems and procedures available.