



The Tape Air Gap

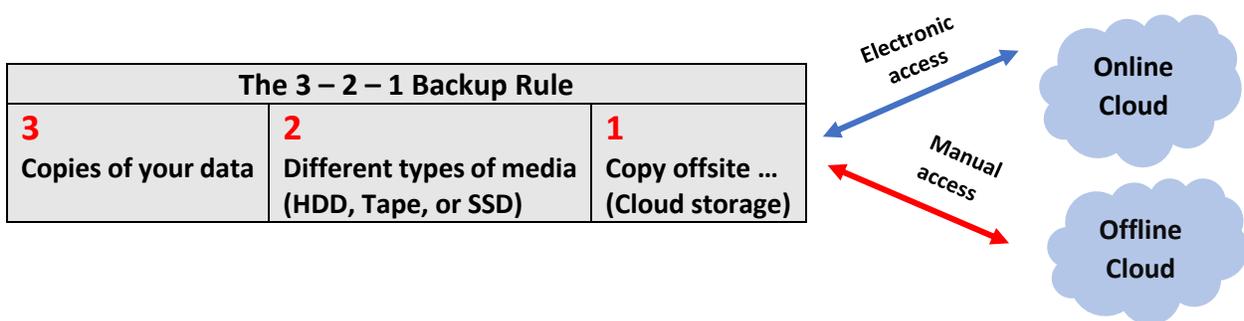
Provides Defense Against Cybercrime



BY: Fred Moore President

www.horison.com

Given the changing landscape of the IT industry, many of the original concepts about backups are delivering additional value and are now back in style. One of those original backup concepts is the 3-2-1 rule. This rule states enterprises should have three copies of backups on two different media types, one of which is kept offsite. There are two ways to have an offsite copy – either with an online (electronic access) or with an offline (manual access) cloud. The offsite *and* offline copy is rapidly becoming more critical and describes is what is now referred to as an “air gap”. An “air gap” is an electronically disconnected copy of data that prevents rolling cybercrime disasters from getting to your all your backup copies. The only way to create a physical air gap is to copy something to removable media and send that media offsite. This means tape media for most all data centers. Off-site backup and storage facility defines can be online or offline and can often be the most physically secure facilities in the industry. These are often built in [solid granite mountains](#), [underground bunkers](#) or other highly discrete locations.

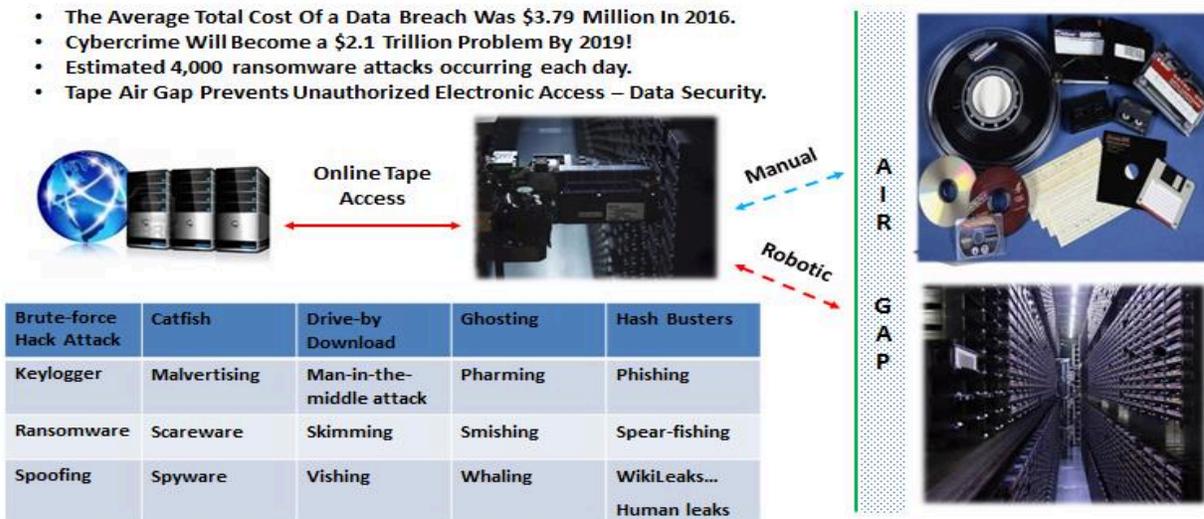


You can put an electronic air gap between your backup server and backup storage by making sure that the backup is not accessible via any network or electronic connection. Most tape cartridges typically reside in library racks meaning they are offline well over 95% of the time (protected by the air gap) and are not electronically accessible to hackers.

The air gap prevents cyber-attacks since data stored offline - without an electronic access - cannot be hacked. For example, Ransomware is latest crypto-viral extortion technique which encrypts the victim's files making them inaccessible, and then demands a ransom payment to decrypt them. These new types of attacks embed time-delayed undetected malware into your backup repositories sometimes taking several months to reactivate. This makes file restoration pointless because as you recover your data, the ransomware re-ignites and then re-encrypts the data all over again. This is known as the [Attack-Loop™](#).

The Tape Air Gap = Data Security

- The Average Total Cost Of a Data Breach Was \$3.79 Million In 2016.
- Cybercrime Will Become a \$2.1 Trillion Problem By 2019!
- Estimated 4,000 ransomware attacks occurring each day.
- Tape Air Gap Prevents Unauthorized Electronic Access – Data Security.



Whether you have the best backup solution, the latest anti-virus protection, or multiple versions of backup repositories, this next generation of cybercrime is evolving so quickly that those concepts seldom matter anymore. In a cloud-based backup, critical data is backed-up over the internet and most likely stored in a shared storage infrastructure at an off-site data center maintained by a third-party cloud company providing backup, archiving and replication services.

Fortunately, [Attack Loop software](#) is becoming available and uses signature-less technology which checks and quarantines malicious code upon entry into the backup repository and again prior to recovery into your environment. Combining offline tape storage with Attack Loop software yields the greatest chance of preventing cybercrime.

Keep in mind that [tape technology](#) is not standing still. IT executives and both online and offline cloud service providers are addressing new applications leveraging tape for its security, air gap cyber protection, and economic advantages. Tape has expanded its position as a highly effective complement to flash and disk for the foreseeable future due to its higher reliability than HDD by three orders of magnitude, higher capacities, much faster data rates, and significantly lower energy costs. The TCO for HDD is typically 6-15x times greater than tape offering significant cost savings. Easy to use [TCO tools](#) are available to determine your specific TCO. This recognition is driving continued investment in new tape technologies defining robust roadmaps that face few limits for the foreseeable future.

Bottom line: Given the rising wave of cybercrime, the role of tape-based offline storage and cloud solutions taking advantage of the “Tape Air Gap” is back in style.