HORISON
Information Strategies

Fred Moore, President
Horison.com

2020 Technology Update Series

THE TAPE AIR GAP

Protecting Data From Cybercrime

The changing landscape of the data protection industry has evolved from primarily backing up data in order to recover from hardware, software, network failures and human errors, to fighting a mounting wave of cybercrime. Over the years, hardware and software have significantly improved their reliability and resiliency levels but security is a people problem, and people are committing the cybercrimes. Cybercrime has now become the biggest threat to data protection and the stakes are getting higher as anonymous individuals seek to profit from other's valuable digital data. With a cease-fire in the cybercrime war highly unlikely, we are witnessing *a rapid convergence of data protection and cybersecurity* to counter rapidly growing and costly cybercrime threats, including ransomware. The growing cybercrime wave has positioned air gapped storage solutions as a key component of digital data protection – they simply can't be hacked.

CYBERCRIME SCENARIO 2020

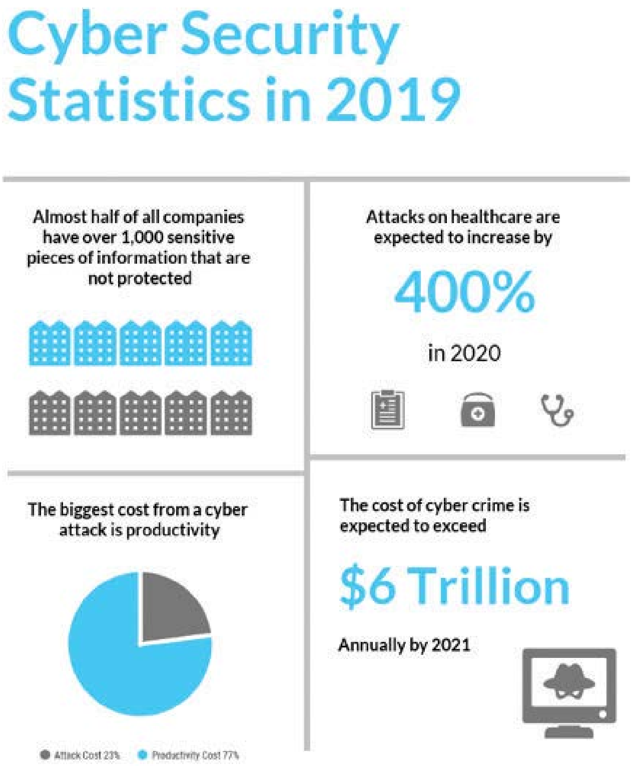
No computer system is immune from cybercrime. Emails deliver over 60% of all cybercrime infections and initially land on your computer's HDDs or SSDs - but not on tape. Vulnerabilities may be uncovered by hackers, security companies, government agencies, software and hardware vendors, or end users. Endpoint security, firewalls, VPNs, and authentication systems are on most every system, but can these security layers really provide the sustainable and bullet proof levels of security your organization needs? Unfortunately, each of these security layers provides hackers with a backdoor directly into your organization. In addition, there are more than 111 billion lines of new software code created each year and the highly hyped IoT is projected to reach over 40 million endpoints by 2025 introducing countless vulnerabilities which can be exploited creating a perfect storm for cybercriminals.

Clearly the magnitude of the potential impact from cybercrime attacks cannot be underestimated and the following statistics bear this out.

- The worldwide spending on cybersecurity is forecasted to reach $133 B by 2022. **(Varonis)**
- URLs embedded in emails remains the number one way for computers to become infected. **(Safety Detectives)**
- Hackers attack every 39 seconds or 2,244 times a day. **(Varoni)**
- By 2020, the estimated number of passwords used by humans and machines worldwide will grow to 300 billion. **(Cybersecurity Media)**
- The average cost of ransomware attacks is $141,000 with $11.5 billion in total damages in 2019.
- The financial services industry has the highest cost from cybercrime at an average of $18.3 million per company. **(Accenture)**
- By 2021, it's projected that there will be 3.5 million unfilled cybersecurity jobs globally. **(Cybersecurity Ventures)**
- Cybercrime breaches are anticipated to increase nearly 70% by 2024. **(Security Boulevard)**
- Cybercrime damage is projected to hit $6 trillion annually by 2021. **(Cybersecurity Ventures)**

Cyber criminals are attempting to capitalize on the increased risks caused by the social adjustment to the COVID-19 pandemic. Many employees are working from home, outside of the traditional office network perimeter, in hybrid WFH (work-from-home) networks. Family members and school children are becoming co-workers by sharing business and WiFi networks in this newly expanded and co-mingled work environment which can easily spread infections to other machines and, sometimes, entire networks. The pandemic has been a boon to cybercriminals, who are having a heyday exploiting numerous security weaknesses to capitalize on people's fears about the virus while pushing security concerns to the endpoints.

Is the hybrid workforce becoming the new normal? Creating a unified cyber infrastructure that's secure across the new hybrid environment is now critical. In the digital world, the focus has been more on trusted devices and IP addresses than validating the actual person behind the screen, but that will need to change. In a new normal, storage related companies will design hardware and software with security in mind, not as an afterthought or add on feature. The emphasis on device security should reach its zenith in an environment where the devices are at the edges and don't have traditional users, specifically from the rapid growth of the IoT **(Internet of Things)**.



Cyber Security Statistics in 2019

Almost half of all companies have over 1,000 sensitive pieces of information that are not protected

Attacks on healthcare are expected to increase by 400% in 2020

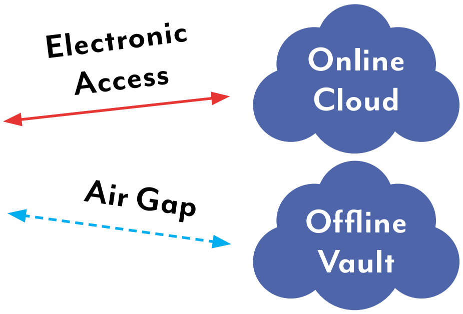
The biggest cost from a cyber attack is productivity

The cost of cyber crime is expected to exceed $6 Trillion Annually by 2021

THE OPTIMAL BACKUP STRATEGY

Backup was the original data protection strategy. Many of the fundamental IT concepts of data backup have expanded their roles cybercrime spreads. Backup is important but having one backup copy is often not enough. The optimal backup strategy deploys the Golden Rule of Backup, the 3-2-1 rule. This rule states enterprises should have three copies of backups on two different media types, one copy of which is kept offsite. There are two ways to store an offsite data copy – either with an online (electronic access) or with an offline (air-gapped or manual access) copy. By keeping backup copies both locally and physically offsite or in the cloud, you double the protection of your data in the event of any unforeseen event or disaster. Both of these approaches may use a data vault or a cloud service provider and both can use the same SSDs, HDDs and air-gapped tape for backup storage, just like a typical data center.

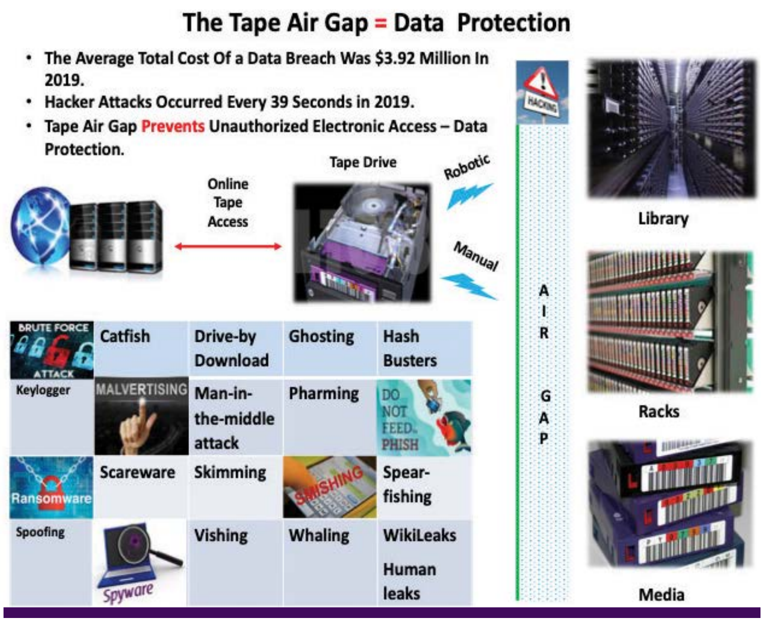
	THE **3—2—1** BACKUP RULE	
3. Copies of data	**2.** Different types of media (HDD, Tape, SSD)	**1.** Offsite Copy Cloud/remote/vault (HDD, Tape)



TAPE AIR GAP PROVIDES CYBERCRIME PROTECTION

Traditional backup and archival data can be stored locally or in cloud environments. In contrast, a cyber-resilient copy of data must meet additional more stringent requirements. This is where "air gapping" and tape technology are gaining momentum. The rise of cybercrime officially makes the offline copy of data stored on tape more valuable and takes advantage of what is referred to as the tape air gap. The tape air gap is an electronically disconnected or isolated copy of data in a robotic library or tape rack that prevents cybercriminals from attacking a backup, archive or any other data. Without an electronic connection to tape (or any other offline media), data stored on tape can't be hacked.

Tape cartridges in a robotic tape library or manually accessed tape cartridges in tape racks, are currently the only data center class air gapped storage solution available. HDDs and SSDs are always online and accessible to hackers and are the initial entry point for cybercrime infections. Tape cartridges are online only when the tape cartridge is mounted in the tape drive. When tape media is not mounted on a drive, it is electronically disconnected from any system and protected from infection by the tape air gap. Note data infected online which escapes firewalls and traditional security prevention techniques can be backed up to tape circumventing the air gap protection. This is a common technique used for ransomware.



The Tape Air Gap = Data Protection

- The Average Total Cost Of a Data Breach Was $3.92 Million In 2019.
- Hacker Attacks Occurred Every 39 Seconds in 2019.
- Tape Air Gap Prevents Unauthorized Electronic Access – Data Protection.

BRUTE FORCE ATTACK	Catfish	Drive-by Download	Ghosting	Hash Busters
Keylogger	MALVERTISING	Man-in-the-middle attack	Pharming	DO NOT FEED PHISH
Ransomware	Scareware	Skimming	PHISHING	Spear-fishing
Spoofing	Spyware	Vishing	Whaling	WikiLeaks Human leaks

ATTACK LOOPS MAKE CYBERCRIME PREVENTION AND RANSOMWARE MORE CHALLENGING

In 2019, 51% of organizations were hit by ransomware and cyber-criminals succeeded in encrypting the data in 73% of these attacks. Though digital extortion is not new, ransomware malware remains a popular crypto-viral digital extortion technique that gets around firewalls and malware protection tools and locks the system's screens by encrypting selected users' files. A ransomware attack typically begins when an end user clicks on a website link or opens a file attachment in a malicious email that is part of a phishing (random) or spear-phishing (targeted) cybercrime campaign.

These attacks embed time-delayed, undetected malware into online files and the malware stays dormant, sometimes taking several months to reactivate. In the meantime, the dormant malware is eventually and unknowingly backed up to a backup device, normally tape or HDDs. In the case of a tape backup device, data is infected online *before* it is copied to tape avoiding air gap protection. After a time-delayed *online* malware detonation disabling the file(s), the pre-attack generation of the backup file(s) is restored only to realize that the recovery data from HDD or tape re-inserts the ransomware back into the system and re-encrypts the data all over again for a perpetual loop of attacks. This makes file restoration pointless because as data is recovered, the ransomware re-ignites. The Attack Loops usually continue until a ransom or extortion fee is paid, typically into an anonymous bitcoin account in exchange for the deciphering key.

Fortunately several enterprise-class anti-ransomware backup software solutions are now available – **see DCIG report**. These solutions identify and quarantine malicious code upon entry into the backup repository and again prior to recovery into the online environment with the malicious code disabled. Coupled with the tape air gap, this provides a strong data protection solution.

SUMMARY

Today's world becomes more interconnected with each passing day. Yet, for all its advantages, this increased connectivity brings a much greater risk of theft, fraud, and abuse. To fight cybercrime, organizations must reevaluate their data protection strategies. If an organization does not have a robust security plan, it had better have a bitcoin account ready to pay the ransom. The tape air gap can become the last line of defense for data protection simply because criminals can't delete or encrypt what they can't access over the network or any other electronic link. Coupled with encryption, WORM, and the tape air gap, tape delivers the highest levels available of hardware data protection. With new security challenges appearing daily, the convergence of data protection and cybersecurity to counter the growing numbers of threats is well underway. Businesses can reduce their exposure cybercrime by maintaining an effective and continually evolving cybersecurity strategy.

Horison Information Strategies is a data storage industry analyst and consulting firm specializing in executive briefings, market strategy development, whitepapers and research reports encompassing current and future storage technologies. Horison identifies disruptive and emerging data storage trends and growth opportunities for end-users, storage industry providers, and startup ventures.