HORISON
Information Strategies

Fred Moore, President
Horison.com

2020 Hyperscale-lite Storage Series

THE TAPE AIR GAP

Protecting Data From Cybercrime

The data protection industry landscape has evolved from primarily backing up data in order to recover from system 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 others' valuable digital data. With a cease-fire in the cybercrime war highly unlikely, we're witnessing a rapid convergence of data protection and cybersecurity to counter rapidly growing and costly cybercrime threats, including ransomware. The growing cybercrime pandemic has positioned air-gapped storage solutions as a key component of digital data protection. The larger the storage environment, the greater the impact of the tape air-gapped data since it simply can't be hacked. Hyperscale-lite (HSL) describes large-scale data centers representing the next wave of hyperscalers and are often Cloud Service Providers (CSPs). HSLs cannot be solely responsible for the security of hundreds of customers' critical data assets. This is a key concern as cyber threats increasingly target data-rich cloud storage environments.

CYBERCRIME SCENARIO 2020

No computer system – from the desktop to the cloud to the future HSL data centers – is immune from cybercrime. Many organizations favor a multi-cloud environment because it allows them to pick and choose their preferred cloud services from different CSPs, but this ever-expanding multi-cloud environment gives rise to new types of risk.

Emails deliver over 60% of all cybercrime infections and initially land on your computers 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 bulletproof 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 a countless number of new vulnerabilities which can be exploited. It's a perfect storm for cybercrime.

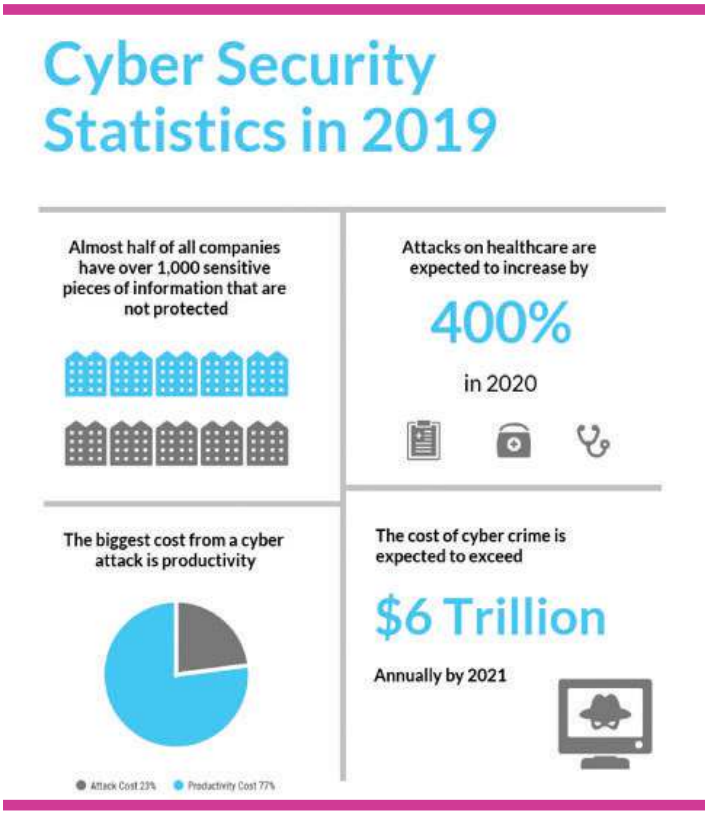
KEY POINT

For HSLs, cloud security relies heavily on the customer's ability to implement the right level of data security controls, particularly with multi-cloud storage solutions.

CYBERSECURITY CHALLENGES MOUNT

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 forecast to reach $133 B by 2022. **(Varonis)**
- URLs embedded in emails remain the #1 way for computers to become infected. **(Safety Detectives)**
- Hackers attack every 39 seconds, or 2,244 times a day. **(Varonis)**
- 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)**



Cybercriminals 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 virus vectors by sharing business and WiFi networks in this newly expanded and co-mingled work environment where infections can easily spread to other machines and, sometimes, entire networks. The pandemic has been a boon to cybercriminals, who are having a heyday exploiting security vulnerabilities to capitalize on people's fears about the virus while pushing security concerns to the endpoints. When the hybrid WFH network is backed up to the cloud, security becomes more complex.

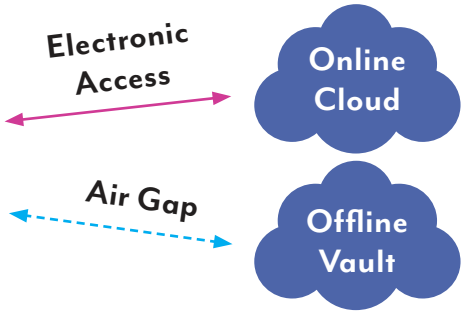
Is the hybrid workforce becoming the new normal? Creating a unified cyber infrastructure that's secure across the hybrid environment is critical. Historically the focus was more on trusted devices and IP addresses than validating the actual person behind the screen, but that will need to change. In a new normal, storage companies will design systems 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 the IoT **(Internet of Things)**.

KEY POINT

Cybercrime challenges continue to increase and pose the biggest threat to stored data. HSLs provide storage services for multiple businesses, raising the stakes to provide a highly-secure storage infrastructure.

THE 3—2—1 BACKUP RULE

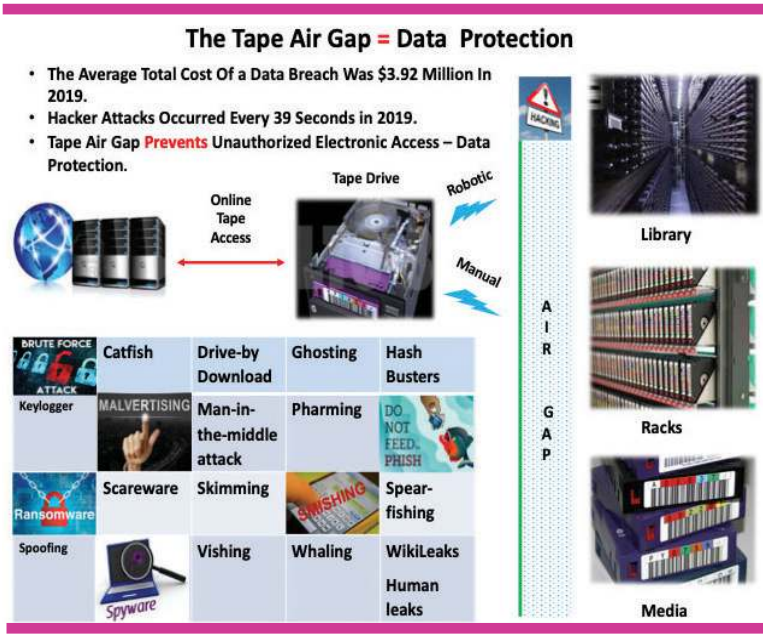
3. Copies of data	**2.** Different types of media (HDD, Tape, SSD)	**1.** Offsite Copy Cloud/remote/vault (HDD, Tape)



THE OPTIMAL BACKUP STRATEGY

Many of the fundamental IT concepts of data backup have expanded their roles as the cybercrime pandemic spreads. Backup is important but having one backup copy is sometimes not enough. The optimal backup strategy deploys the Golden Rule of Backup, the 3-2-1 rule.

This rule states that 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. Each of these approaches may use a data vault or a cloud service provider and both options can use the same SSDs, HDDs and air-gapped tape for backup storage, like a typical data center.



TAPE AIR GAP PROVIDES CYBERCRIME PROTECTION

TTraditional backup and archival data are normally 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 protecting the offline or cloud copy of data stored on tape more critical, and describes what's 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 other data copy. Without an electronic connection to the network, data stored on tape can't be hacked. In addition, tape offers WORM (Write Once Read Many) functionality typically for archival data, which once written, cannot be modified. This write protection affords the further assurance that the data is immutable and cannot be tampered with once it is written to the device.

Tape cartridges in a robotic tape library, or manually accessed tape cartridges in tape racks, are currently the only available data center class air-gapped storage solution. 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 by the tape air gap. HDDs and SSDs are always online and accessible to hackers, and are the initial entry point for cybercrime infections. CSP and HSL data centers can provide immediate protection by implementing tape systems for backup and archival data. Customers can request air-gap protection (tape) to ensure the highest protection services from their CSPs.

KEY POINT

Only with a proactive disaster recovery plan can the growing HSL businesses increase their chances of withstanding a ransomware attack. Implementing a tape air gap storage system is the easiest way to add cybercrime security.

ATTACK LOOPS MAKE CYBERCRIME PREVENTION AND RANSOMWARE MORE CHALLENGING

Digital extortion is not new and 50% of 582 cybersecurity professionals surveyed in 2019 do not believe their organization is prepared to repel a ransomware attack. (Source: Pwnie Express)

Ransomware is a popular crypto-viral digital extortion technique that gets around firewalls and malware protection tools, locking 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, HDDs, or the cloud. After a time-delayed online malware detonation disabling a file(s), the pre-attack generation of the backup 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, Attack Loop prevention software is becoming available to 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. Advanced Attack Loop software is just beginning to use automated, self-learning AI and ML strategies to improve detection capabilities and, coupled with the tape air gap, provides the best option to prevent attack loops. Expect significant advances in this software technology in the coming years, tightly integrated with cybersecurity software to disarm any ransomware.

For HSLs and CSPs, the cloud storage infrastructure is not inherently immune to ransomware. As ransomware attacks increase, customers are wondering what they can do to protect themselves. As a natural response, cloud storage and backup vendors are positioning attack loop prevention software and hardware tape air-gapped technology as a solution to the ransomware threat.

KEY POINT

Ransomware attacks have increased over 97% in the past two years. (Source: Phishme) Taking advantage of the tape air gap, and attack-loop prevention software, adds another line of defense against cybercrime.

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, HSLs, CSPs, and ALL organizations must reevaluate their data protection strategies. Ideally an air-gapped solution will be an integral component of that strategy. If an HSL or CSP doesn't have a robust security plan, it had better have a bitcoin account ready to pay the ransom. The tape air gap can be 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. Combined 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 to it 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.