HYCU

EBOOK

5 steps every IT professional should take to prepare for a ransomware attack.

Steps to prepare for a ransomware attack.

"As much as all of us in technology would like to believe we can eliminate ransomware attacks, the focus needs to be on rallying the industry around a way of quantifying and measuring what steps can, and should, be taken to avoid having to pay exorbitant transoms for companies to get their data back." *Simon Taylor, Founder and CEO, HYCU, Inc.*

As IT migrates from data centers to hybrid cloud environments, organizations have to take a hard look at their infrastructure and identify the different ways to approach, manage and modernize their multi-cloud ransomware recovery efforts.

The convergence of threats, heightened by ransomware and phishing tactics as well as working collaborations amongst cybercriminals has cemented the need for organizations to start making better choices when it comes to their ransomware readiness strategy.

Threat actors show no prejudices when it comes tocompany size or industry vertical. According to IDC's "2021 Ransomware Study", approximately 37% of global organizations said they were the victim of some form of ransomware attack in 2021. And, to add fuel to the fire, it is estimated that **cybercrime will cost** the world $10.5 trillion annually by 2025. Both reactive and proactive approaches should be taken to protect, detect and recover from these attacks.

This eBook highlights 5 best practices for IT professionals to adopt to make backup and recovery a central part of any ransomware threat mitigation approach.

Because, it's not a matter of "if" an asttack will happen, but "when".

Leave no application unprotected.

Multi-cloud is a reality now for most organizations and managing the movement of data between these cloud environments is critical. However, for some, there is still an over-reliance on legacy and poorly functioning IT systems which leaves hypersensitive data vulnerable and an appealing target to cybercriminals. Protecting data and applications with a proven multi-cloud backup solution to keep it safe and secure is imperative.

This sounds very simplistic; however, this is a struggle for most businesses. Traditional backups will discover all the virtual machines and containers, but without the context of an application, IT teams may not know what the are backing up. Is data application consistent? What is the context of the application that is being backed up? VM's are great, but how does IT ensure they have an application-consistent backup or application- aware backup. The bigger question is can this all be done automatically without having to add manual tasks? Simply put, IT teams need to make sure it is automated as much as possible without adding manual intervention.

Secondly, the reason people implement backup is to help with recovery in the case of human error or in the event of a disaster. What needs to be considered is "how long is it going to take to recover any data?" Can

current software ensure a fast recovery? A smart system should have the ability to automate how long a system will be down and how long it will take to be up and running again. This is referred to as Recovery Time Objective (RTO).

Finally, are systems compliant with automation policy? Can systems tell if they are compliant? IT teams will sleep better at night knowing that data is safe and easily recoverable. Systems should be fully compliant with policies that allow for automatic recovery.

Systems should be fully compliant with policies that allow for automatic recovery.

Air-gapped backup security and backup integrity.

To be “all-in” on ransomware protection, include an air-gapped backup solution.

As ransomware threats continue to grow around the world, there has been much buzz generated around the topic of air-gapping and what it means to an organization's overall backup and recovery strategy? So, what does it mean? Simply put, an air-gapped backup, included in many backup and recovery strategies, is a unique technique used to prevent data loss by copying an organization's data when it's offline and inaccessible. When a computer network or device is detached from the public internet or a LAN, it's impossible for a backup device to be hacked or compromised remotely.

How To Protect Infrastructure?

Without an air-gapped backup, any organization's data protection strategy is at risk. There are three fundamental solutions to choose:

01 Native IAM support. (Identity and Access Management)

Integrate and inherit all the platform's security policies to ensure zero security loopholes all without constantly redefining user permissions.

02 Secure integration with any platform.

Make sure to leverage best-practice standards to integrate with all on-premises and public cloud platforms in a secure and timely manner.

03 Backup network segmentation.

Isolate backup data and backup management traffic from production environments for total air-gapped backup security.

The bottom line is that air-gapped backups provide an extra layer of protection against bad actors and are a powerful defense to combat ransomware.

If an organization is "all-in" on its ransomware protection strategy, it must include an air-gapped backup solution.

To be "all-in" on ransomware protection, include an air-gapped backup solution.

Back up or archiving data onto air-gapped/ worm storage.

To minimize ransomware threats and maximize protection, storage is your best line of defense.

WORM is the only option that offers protection right where the data lives.

What is WORM storage and why is it important to any data protection strategy?

WORM (write once, read many) storage is a method of storing data so it cannot be altered or deleted once it has been written. This means that data is "immutable" to any outside actors that might want to gain access to, tamper with or erase data altogether. Think of WORM data storage as a Polaroid picture: a snapshot of data that has been cemented in time. Look at that picture many times, but it can never be overwritten, deleted or manipulated in any way.

Furthermore, WORM storage is scalable at a pace that keeps up with data's unwieldy rate of growth. According to a recent report by Statista, 74 zettabytes of data were created globally in 2021. (a zettabyte is a trillion gigabytes). As volumes increase, so does the importance of keeping your critical data secure.

WORM storage is the easiest and most effective strategy against ransomware.

When implementing any form of backup solution–cloud, on-prem, or hybrid–organizations should look for all the following:

01 WORM-based immutable backups:

Perform backups, copies, and archives to WORM-enabled object storage to shield them from ransomware.

02 WORM immutable backups for all:

Perform WORM-enabled backups of all hypervisors, NAS Buckets, and physical servers.

03 Choice of WORM backup targets:

Leverage on-prem and cloud-based WORM-enabled object storage.

To minimize ransomware threats and maximize protection, storage is your best line of defense.

WORM is the only option that offers protection right where the data lives.

Create a cost-effective ransomware ready DR strategy.

Every ransomware situation is different in terms of network capabilities, security capabilities, and most importantly backup and recovery capabilities.

The expression is tireless. It's not a matter of "if", but a matter of "when." Ransomware attacks happen, it's inevitable. Unfortunately, cybercriminals are not biased towards company size and any business is vulnerable; large, small, and mid-market companies are all equally at risk. A solid backup and recovery strategy ultimately saves time by negating the need to pay the ransom and reducing downtime from days to minutes.

One major misconception when it comes to backing up on public clouds is that it is automatic. Companies like Google, AWS and Azure do a fantastic job of storing critical data, but ultimately the company is responsible for the protection, detection, and recovery (PDR) of data. It's called "shared responsibility."

And, just as important as the protection and detection of data is, recovery is often the most overlooked–and possibly most important–part of disaster recovery strategies.

"What really matters is recovery. You can't run your business if your data is not available." *Enrique Salem, Partner, Bain Capital Venture Partners*

The importance of implementing a cost-efficient and effective ransomware-ready DR strategy based on industry best practice cannot be overstated It allows organizations to not only plan for but measure readiness. With it, IT teams can successfully respond to, mitigate and recover from a ransomware attack to protect critical business operations, customer and employee sensitive personal data, and other confidential and proprietary information. Here are some essential capabilities that any company will need to consider:

01 **Ability to go back in time.**

02 **Efficient recovery options from offsite copies.**

03 **Flexible recovery options at anytime.**

04 **Recovery into public clouds.**

Periodically assess ransomware readiness.

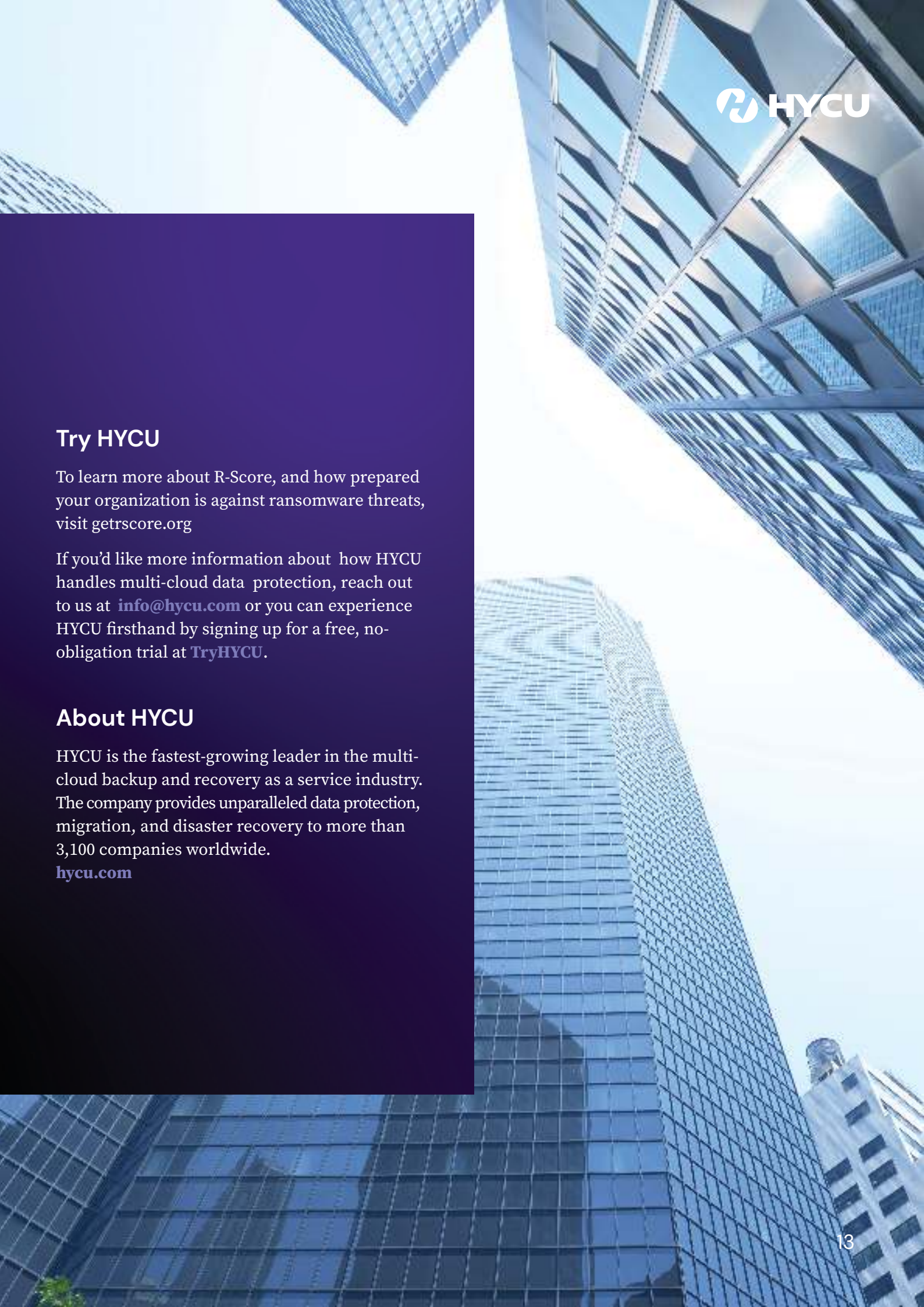
Now that a cost-effective ransomware-ready DR strategy is in place, ask yourself this one question:

How efficient is the ransomware protection and recovery strategy if there is no ability to assess readiness periodically?

As mentioned earlier, cybercriminals are becoming increasingly clever and changing their tactics to leverage current conditions and compel quick action. This behavior has taught organizations to be more vigilant with their approach. However, in many instances, we have all become too complacent with our preparedness. The ever-present news coverage and media exploitation of impactful ransomware attacks globally has left us "desensitized" to the thought of being victimized. In turn, this has caused users to become lax in keeping track of emerging threats and security teams may choose not to take action to strengthen their digital safety.

This is exactly why HYCU and its partners developed R-Score, a first-of-its-kind assessment tool designed to help companies prepare to recover from an inevitable ransomware attack. Built from 5 main categories, R-Score will assess how well prepared any organization is to handle cyber and ransomware threats. Similar in nature to a FICO score, R-Score is based on a scale from 0-to 1000. The higher the score, the better prepared an organization is to recover from an attack. Additionally, it provides recommendations on how to improve an organization's overall readiness.

"The narrative is clear, malicious cyber-criminals will continue to find lucrative and creative paths to hit you with a ransomware attack." *Simon Taylor, Founder and CEO, HYCU, Inc.*



Try HYCU

To learn more about R-Score, and how prepared your organization is against ransomware threats, visit getrscore.org

If you'd like more information about how HYCU handles multi-cloud data protection, reach out to us at **info@hycu.com** or you can experience HYCU firsthand by signing up for a free, no-obligation trial at **TryHYCU**.

About HYCU

HYCU is the fastest-growing leader in the multi-cloud backup and recovery as a service industry. The company provides unparalleled data protection, migration, and disaster recovery to more than 3,100 companies worldwide.
hycu.com

27-43 Wormwood Street Suite #650, Boston MA 02210, USA | Phone: +1 617 681 9100 | E-mail: Info@hycu.com |