HYCU

EBOOK

Accelerating your ransomware recovery with the right backup strategy.

How long will it take you to get back to business?

Introduction.

For those companies that fall victim to a ransomware attack, the aftermath can be challenging and painful. Over the last few years, more companies have paid the ransoms to attackers (26% paid in 2020 and 32% in 2021), but only 8% of those companies managed to get back all their data. Beyond the ransom, the cost of remediating what's lost, including downtime, lost orders, operational costs, and more, has doubled from an average of $761,106 to $1.85 million in 2021. Source: Sophos Press Release

It's said that an ounce of prevention is worth a pound of cure and that adage seems to hold true in the world of corporate cybersecurity:
much of the focus of IT and security teams revolves around the detection of and protection from ransomware attacks. But even the teams most prepared to fend off an attack might not be prepared to get the business back up and running quickly.

It's important for companies to prepare for a ransomware-specific data recovery strategy because, statistically speaking, it's a matter of when a company will be hit by ransomware and not if they will be. At a time when companies operate in multiple clouds and have legacy on-premises infrastructure to back up, preparing to recover data and return to business requires a deliberate approach to ransomware recovery. Just because your data is in the cloud doesn't mean you could recover it —and the applications, VMs, etc.— and be back up and running without days or weeks of work.

That's why you need a ransomware recovery strategy that focuses on reducing the time between the intrusion being detected and your applications and data being restored. Not only will this lower the costs associated with remediation, but it will reduce the pressure companies feel to pay to get their data back.

Despite the increasing threat of ransomware and exponential increases in data being generated, IT teams have not made a corresponding increase in their backup and recovery investments. From 2020 to 2022, IT spending on backups and disaster recovery has stagnated at 8% of the budget.

In this environment of increased risk and stretched budgets, what do you need to know to evaluate your ransomware recovery preparedness? We'll look at 5 key areas to consider if your IT and security goals include rapid ransomware recovery.

Best practices for ransomware recovery preparedness.

Any ransomware recovery strategy requires an honest assessment of the backup and recovery capabilities of the organization. As IT infrastructures evolve to become more reliant on cloud computing and data storage, for example, companies may become lax in their recovery preparedness by assuming that cloud storage inherently includes recoverability.

While companies are aware of the need to prevent and detect cyber threats and work diligently to educate and prepare the broader organization to fend off attacks, it takes a dedicated approach to develop a ransomware specific recovery plan.

Traditional disaster recovery plans will get you part of the way there, but ransomware preparedness should focus on getting back to business without losing business continuity. Organizations need to evaluate five key areas so they can create backups that are safe and reliable in the event of an attack.

We'll dive deeper into each one in a moment but taken altogether these areas comprise the backbone of any ransomware recovery strategy. A ransomware recovery-specific approach to each area differs compared to

your raditional disaster recovery. Relying on snapshots alone, for example, is not enough because they're not a good long-term solution since ransomware can lay dormant for up to six months in your systems. It's easy to see why a comprehensive backup and recovery strategy for ransomware is critical and distinct from other disasters which happen in the moment.

Our lens here is towards creating a ransomware recovery strategy that prioritizes a swift return to normal business operations. To do that, it requires immutable, application-consistent backups that can be recovered onsite or offsite in hours, not days or weeks.

Let's take a closer look at each of the five key areas to consider in your ransomware recovery strategy.

The five key areas to consider are:

01 Backup process.

02 Backup infrastructure.

03 Secutity and networking.

04 Restoration assurance.

05 Disaster recovery (DR).

Backup process.

How often and how much you back up your data should constitute the service-level objectives (SLOs) agreed to by stakeholders' business requirements and the IT team. This SLO should be measured by KPIs like recovery point objectives (RPOs) — how much data you're willing to lose determined by intervals between backups — and recovery time objectives (RTOs) — how quickly you can recover information and applications in the event of a disaster.

When building out your ransomware recovery strategy, your RPOs and RTOs should be calibrated to your businesses needs and any applicable industry standards. Beyond that, your targets for recovery time and data loss are determined by the costs of managing the backups versus the risk of data loss. Changing how frequently you back up, how you back up your data (fully, differentially, or incrementally) and the data storage targets for your backups (local storage like tape or disk, cloud, etc.) will determine whether you can hit your SLOs and stay under budget.

Will you hit your SLOs and stay under budget?

Determining factors:

01 How frequently you back up.

02 How you back up your data.

03 Data storage targets for your backup.

3–2–1 rule.

One standard to adopt for your organization to protect against the risks of a lengthy ransomware-based interruption is the 3-2-1 rule. The rule states your data should be backed up three times, on two different media (on an appliance and in the cloud, for example) with at least one backup offsite.

Air-gapped and immutable backups.

When it comes to ransomware recovery, it's critical to ensure one copy of your data is inaccessible to the threat as a last resort when your other measures fail. There are two ways to account for this: air-gapped and immutable backups. Air–gapping your backup means creating an offline copy that cannot be accessed through the Internet or a LAN. Combined with immutability — the inability to change data once it's been written — you've got a recoverable backup as secure from ransomware as possible.

Backup Methods for Ransomware Recovery.

Air-Gapping.

Creating an offline copy that cannot be accessed through the internet or a lan.

Immutability.

The inability to change data once it's been written.

Backup infrastructure.

The infrastructure underpinning your ransomware recovery strategy will play a big part in determining the scope and costs of your efforts. There are three types of infrastructure to consider, each with their pros and cons: software, appliance, or BaaS.

These are broad categories, however, and there is certainly an overlap in the infrastructure. For example, you can have software-based virtual appliances.

When it comes to ransomware backup and recovery, you're likely going to take a hybrid approach to meet the 3-2-1 Rule. But where you place your last line of defense — the immutable, air-gapped backups — is critical to ensure rapid onsite or offsite recovery to get the business backup and running within the parameters of your RPOs and RTOs.

01 Software.

With in-house deployment of backup software, companies place backups on their virtual or physical servers. While this can give you control over your backup and keep data in house, the need to constantly update each server manually is a drawback for larger companies. Plus, it doesn't address the 3-2-1 rule discussed earlier, making it a less reliable choice for ransomware recovery.

02 Appliance.

Third-party appliances are a turnkey solution that combine the software and hardware components necessary to back up data within one device. Like the software solution, it gives you the ability to "own" your backup, but with that comes all the maintenance and support required as you manage daily backups. If you're relying on an appliance-based backup strategy for your ransomware recovery plan, consider whether you can make air-gapped backups work here as well.

03 Backup as a service (BaaS).

With BaaS, companies have automated, no-maintenance backups with more flexibility to scale up and down without the hassle of adding more agents or physical servers. When used for immutable off-site backups, it can make recovery in the case of ransomware much faster and simpler than other options. Of course, with this choice you'll have to find the right vendor that supplies all the right requirements.

Security and networking.

"A common misconception is that a recovery plan for ransomware recovery and a traditional disaster recovery plan are the same. The plan many companies have to recover in the event of a natural catastrophe or another type of incident or malfunction is, often, the same one they use to respond to a ransomware attack. This is a compounded disaster waiting to happen; these two things are not the same. All recoveries are not created equal." *Subbiah Sundaram, VP, Product Management at HYCU*

Even the best backup and recovery strategy can falter when it isn't paired with strong security and networking practices and protocols. Like other parts of your network and infrastructure, you need layers of security around your backups to ensure the don't fall prey to cyber thieves if your production environment does.

Adding more security to your backups can add to the costs of infrastructure and administrative time spent, but it's a small price to pay to avoid catastrophic losses of data and business operations. As cyber criminals become more sophisticated in their attacks, backups have become common, if opportunistic, targets, with criminals hoping to increase the likelihood of a ransom payment.

When it comes to securing your backups against ransomware threats, there are several things to consider.

Who has access to your backups?

Cyber threats and ransomware can enter your systems many ways, including by stealing user credentials to key systems and applications. Wherever your backups exist, they should be protected by multi-factor authentication, which makes it more difficult for bad actors to gain access to your backup infrastructure.

How are your backups tied into the broader network?

Secure backups require layers of separation from potentially compromised production environments. Segmenting your network can help isolate backups in the case of an attack and ensure their integrity when you move to restore your data. Similarly, don't duplicate credentials across backup and production environments.

Are your backup targets visible?

Out of sight, out of mind. Wherever your backup target exists, it should not be publicly visible or accessible. It's a simple change that reduces the surface area of any cyber threat.

Restoration assurance.

Your ransomware backup and recovery strategy is not a set-it-and-forget-it deal. Prior to any cyber-attack, you want to ensure that your team has optimized the restoration process, understood its limitations, and tested the capabilities of your data restoration.

Of course, while we talk about "restoring data," what we also mean is restoring your applications and virtual machines. Getting your data back is only useful if it has the context of those applications, and that will greatly decrease the time it takes to get back to business.

As you're evaluating your restoration process, there are a few things to consider:

"You need to ensure you can recover in a timely manner. The executive leadership team and Board of Directors want to know when the business will be back up and running. With the average time to recover from ransomware as long as two to three weeks, the quicker you can recover, the quicker you can repair the damage to your company's business and reputation." *Subbiah Sundaram, VP, Product Management at HYCU*

01 Are agens required?

Agents, or connectors, are sometimes required to administer software-based backups. For large organizations, the need to restore agents prior to application and VM restoration can significantly slow down a return to business.

02 What role will snapshots play?

Snapshots are a great innovation that can speed up the time to restoration. Hypervisor and storage level snapshots can play a key role in your restoration strategy but aren't a substitute for a full-fledged backup strategy since ransomware exposure can compromise systems far beyond the lifespan of a snapshot.

03 Are you verifying your backups?

Your recovery is only as certain as the quality of your backups. Verifying your backups is a critical step to ensure the health of your ransomware recovery strategy. Whether it's a manual spot check of files or running a built-in/third-party health check, you should ensure the integrity of your backups before you need them.

04 Are you testing your restoration process?

It's also important to have a clear benchmark for your restoration process. Testing how long it takes to go from a bare server to running applications again can help you decide whether you're ready to meet ransomware threats head-on, and whether you'll be able to meet your SLOs.

Not all data is created equally.

After an attack, how do you get back to business without trying to boil the proverbial ocean? Consider the importance of the data and applications you've backed up and restore in a logical fashion according to your business' needs.

Start with core infrastructure like Active Directory and DNS that are essential for any of your other applications or services.

Categorize or tier your applications and data and restore in order of importance.

Align SLOs for the different data tiers and match them up with your business objectives.

Disaster recovery.

Like many areas of life, the adage "Prior preparation prevents poor performance" applies to your disaster recovery strategy. The middle of a ransomware attack is not the time to test your disaster recovery strategy.

For ransomware recovery, make sure you have considered the following elements to create the best strategy. Each one has a cost, in terms of time or money, but should be discussed as part of a ransomware recovery strategy.

01 A written disaster recovery plan, with scenarios including ransomware and natural disasters gamed out.

02 Scheduled updates to your disaster recovery plan to account for changes in your business needs and IT environment.

03 An offsite location (hot or cold) chosen in case of disaster recovery.

04 Alternatively, to reduce costs, consider a public cloud location for your disaster recovery environment.

05 A backup environment ready to host recovered servers and applications to reduce downtime.

The importance of fast application and data recovery during a ransomware attact.

Diligent backup protocols and the ability to rapidly restore when you're locked out can get you back to business sooner and cut down on the high cost of lost business.

Ransomware attacks can happen to anyone at any time. When a French construction equipment retail and rental company was hit by a ransomware attack, their ransomware recovery strategy was put to the test.

The attack occurred as they were transitioning from a legacy three-tier VMware environment to a new Nutanix hyperconverged infrastructure (HCI) using AHV and HYCU for backup and restore.

One Sunday morning, the company's IT manager started receiving alerts showing suspicious activity in the system infrastructure, which turned out to be a ransomware attack that had encrypted the servers with a cryptolocker. Despite multiple layers of security, the virus got in through a computer under configuration prior to being ready for production.

The cyber thief demanded several hundred bitcoins, equal to hundreds of thousands of Euros. Instead, after shutting down the servers to limit the spread of the virus, the IT manager turned his attention to restoration and recovery. With the help of the IT team and HYCU support, the company began restoring from local snapshots on the Nutanix cluster, quickly bringing VMs back online and into a new production environment.

While the normal recovery time from a ransomware attack is days, if not weeks, this company had their infrastructure back up and running normally within five hours on a weekend. Thanks to their fast detection of the virus and their commitment to a ransomware-ready backup and restoration strategy, the company was able to avoid any business disruption—and avoid paying a costly ransom.

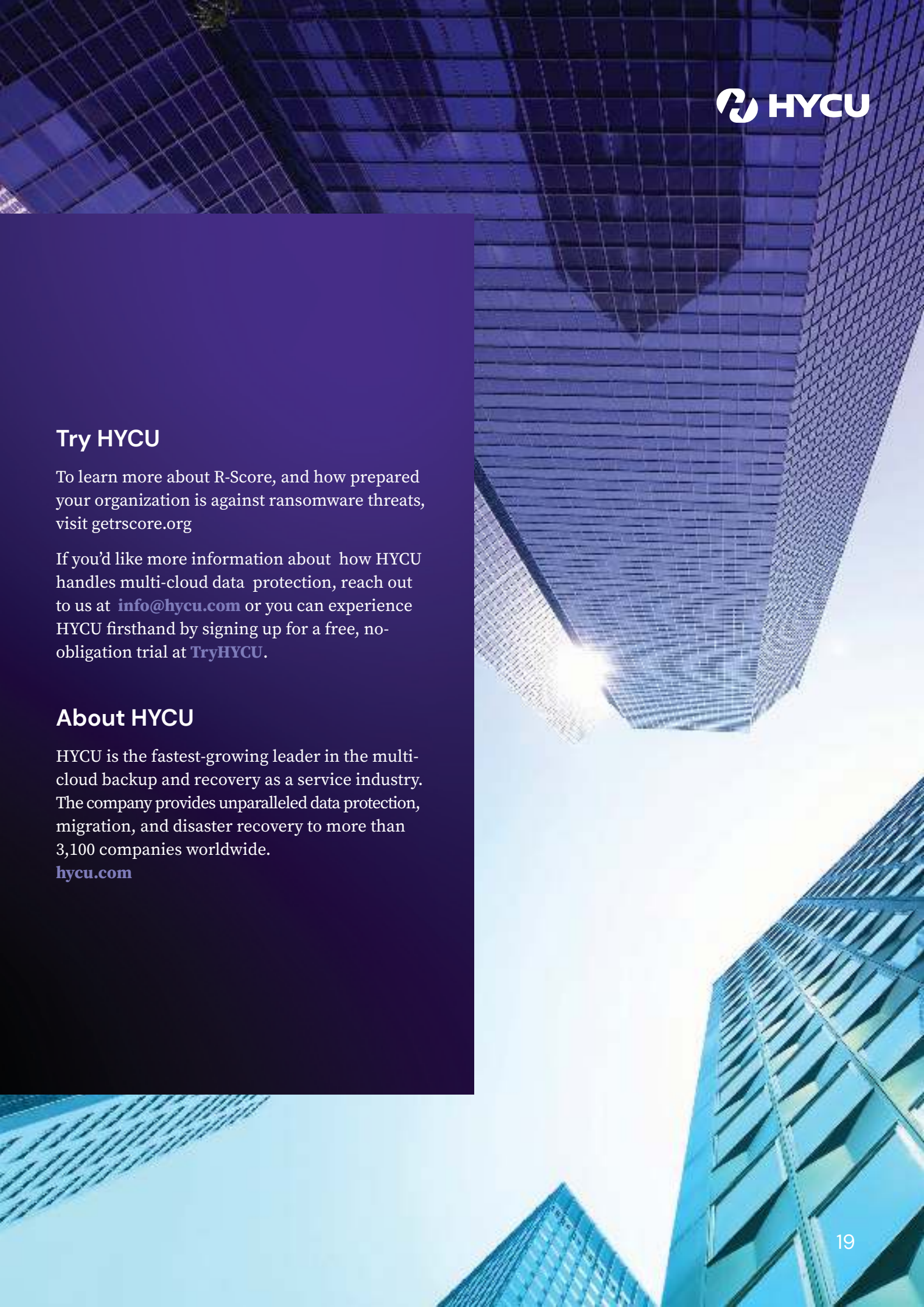
Do you know your R-Score?

Security teams work tirelessly to protect the business from cyber threats. From constant patches and hotfixes to regular cyber threat awareness trainings for employees, preparing for ransomware requires constant vigilance. Your ransomware recovery strategy should follow a similar cadence, with constant monitoring and measuring of capabilities and preparedness.

The best way to do this (and communicate it with key decision makers) is to use the R-Score, an independent self-assessment designed to rate your organization's recovery readiness in the event of a ransomware attack. The score, which works like a credit score to quantify your risk on a 1-1000 scale (with 1000 representing the most prepared), gives your organization an at-a-glance benchmark to track your preparedness as you work to refine your ransomware recovery strategy.

UNPREPARED		PREPARED
0	R-Score	1000

Visit getrscore.org and measure your company's readiness for a ransomware attack.



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 |