HYCU R-Score: Independent Assessment Tool Measures Ransomware Recovery Readiness

By DCIG President & Founder, Jerome Wendt

Every organization has minimally heard about ransomware and too many have been affected by it. However, knowing how best to shore up your internal data protection and recovery solutions to defend and recover from ransomware presents major challenges. The HYCU R-Score survey addresses these concerns. Organizations may assess their ransomware readiness preparedness capabilities in about 15 minutes. Once completed, organizations get a list of key vulnerabilities and steps they can take to counter ransomware's impact.

COMPANY

HYCU, Inc.
109 State Street
Boston, MA 02109
(857) 991-1444
hycu.com

CHALLENGES

- Ransomware will eventually circumvent cybersecurity defenses
- Identifying missing data protection and recovery solutions
- Identifying inadequacies of existing data protection and recovery solutions
- Prioritizing where to begin to shore up internal infrastructure

SOLUTION

HYCU R-Score

DIFFERENTIATORS

- Knowledgeable individual can complete survey in ≈15 minutes
- Freely available with no hidden gotchas or unexpected sales calls
- Generates a score that provides a general sense of an organization's preparedness
- Identifies key data protection and recovery vulnerabilities
- Offers suggestions to fortify the IT environment

Today is the Day

Not next year. Not next quarter. Not next month nor even next week. Today is the day every organization should begin preparing for a ransomware attack if it has not already done so.

Recent and ongoing ransomware attacks provide ample warning to organizations that fail to act. Any organizations that hesitate better count the cost of their inaction. Consider:

- Those that supply software to other providers affected by ransomware may see ransom demands over ten million dollars.
- Large organizations affected by ransomware routinely report paying ransoms in the millions of dollars, or more.
- Even small businesses may pay ransoms of tens of thousands of dollars.[1]

Aggravating these results, these published ransoms do not factor in any of an attack's "soft costs." Recovery time, lost employee productivity, delayed or lost sales, and unrecoverable data all add to ransomware's total cost. These factors collectively argue for the need for organizations to acknowledge ransomware's threat and brace for an attack.

Honest Assessments Precede Comprehensive Defenses

Most, if not all, organizations, have cybersecurity software in place to prevent ransomware attacks. However, as many organizations know, ransomware circumvents these defenses. If bypassed, organizations must have data protection and recovery mechanisms in place. These serve to help repel the attack and recover from it, if necessary.

While many organizations do already have data protection and recovery measures in place, they must quantify if they work. This requires they assess the capabilities of these solutions and how well they position them to recover.

This dictates they perform an honest and thorough assessment of their backup and recovery capabilities. They must ask the right people in their organization the right questions. Should these individuals not know the answers, they need to know where to find the answers or who to consult.

Even should an organization ask the right questions and answer them, they still need to interpret the results. They must appropriately score and weight the responses to identify gaps and strengths. Finally, they must prioritize next steps based upon their findings.

Pulling all these pieces together—the questions, the answers, the scoring, and task prioritization—rarely happens in most organizations. This gap creates the need for a tool that organizations may use to assess their ransomware recovery readiness

HYCU R-Score

HYCU R-Score (short for Ransomware Recovery Score) represents a first of its kind assessment tool that scores organizational ransomware recovery readiness. Organizations access the HYCU R-Score through an online web portal. An individual only needs to access the website to start the survey. The tool then uses entered data to assess their organization's preparedness to repel and recover from ransomware attacks.

1. https://apnews.com/article/joe-biden-europe-government-and-politics-technology-business-88c51d8041b1afdd42fa9f571c3de446. Referenced 7/13/2021.

The Need for a Ransomware Recovery Readiness Score

Everyone fundamentally understands scores and how they work: the higher the score, the better. Scores help everyone quickly and easily assess specific situations and set expectations.

Using a third party to perform this evaluation and generate the score follows precedent. Consider how banks work. As lenders, they do not maintain credit histories for applicants. Rather, they rely upon credit bureaus such as Equifax, Experian, and TransUnion to perform this task. These agencies maintain credit histories, evaluate them, and generate scores that reflect each applicant's credit worthiness and risk.

As ransomware spreads, management, auditors, insurers, and perhaps even investors need a similar independent metric to assess corporate risk. A score reveals how well an organization has prepared itself for a ransomware attack.

A third-party score objectively assesses organizational readiness should a ransomware attack occur. Further, it helps identify strengths and weaknesses. These, in turn, help organizations prioritize the areas, if any, in which they must improve.

Survey Structure

In developing the questions in this survey, HYCU consulted with data protection and security technical architects and experts. These included experienced end-users, analysts, in-house staff, and staff from technology providers. This survey asks about and measures key factors that most heavily influence ransomware recovery readiness.

HYCU similarly drew upon the collective expertise of these individuals to create and weight each question's responses. These weighting generate a final score to provide organizations a sense of their level of preparedness.

The survey currently consists of just over 20 questions with about five questions in each of the five sections. These sections consist of and measure the following:

- ***Backup process.*** These query how well each organization's service level objectives (SLOs) align with their current backup practices. They ask about backup storage locations and organizational change control management.
- ***Backup infrastructure.*** Backup server configuration, management, protection, and recovery along with backup agent requirements are examined here.
- ***Security and networking.*** Organizations get queried on their identity access and management (IAM) and network segmentation practices.
- ***Restore processes.*** These questions examine how frequently organizations verify backups, restores, and their dependencies on specific hypervisors or storage arrays.
- ***Disaster recovery (DR).*** This section asks about whether a DR plan exists, the sites available for DR, and the configuration prerequisites for DR.

Completing the R-Score Survey

To complete and evaluate the R-Score survey, DCIG engaged an individual who works at a major Midwestern insurer. This individual primarily leads the insurer's cloud and cloud DR initiatives. He also possesses knowledge about its day-to-day backup, DR, networking, recovery, and security practices.

Backup Processes

The first survey question asked how well backup SLOs aligned with business SLOs. It defined *'backup SLOs'* in the context of recovery point objectives (RPOs) and recovery time objectives (RTOs). This definition helped us in answering this question.

The next one asked about the percentage of data stored on different media. The survey thankfully defined its use of "different media." Since we were evaluating backups for applications and data hosted in the cloud, we answered accordingly.

The question on immutability and air-gapped data stores prompted some discussion. His cloud-based applications store data on AWS S3 object storage with versioning turned on. This option natively makes data stored on object storage immutable.

However, the institution's on-premises applications primarily store data on disk. He was unsure what percentage of that backup data got stored in an immutable format or was air-gapped after backup. We made an educated guess on the overall percentage of data the company stored in either of those two formats.

The remaining questions focused on change control which we answered in the affirmative.

Backup Infrastructure

These questions were straight forward in asking about backup frequency, the use of backup agents, data encryption, and backup server RPO. We thought the data encryption question seemed better suited for the Security and Networking section. However, we could understand why it is listed here if companies want to encrypt backup data in-flight.

This section did ask for more details about the backup software itself than we anticipated.

For instance, it asked how many physical or virtual servers the organization used to host its backup software. This was tough to answer. The company uses a backup SaaS (software-as-a-service) solution to protect its cloud-based applications. It also uses a separate solution for its on-premises applications. Since the survey only gave us one answer option we chose SaaS.

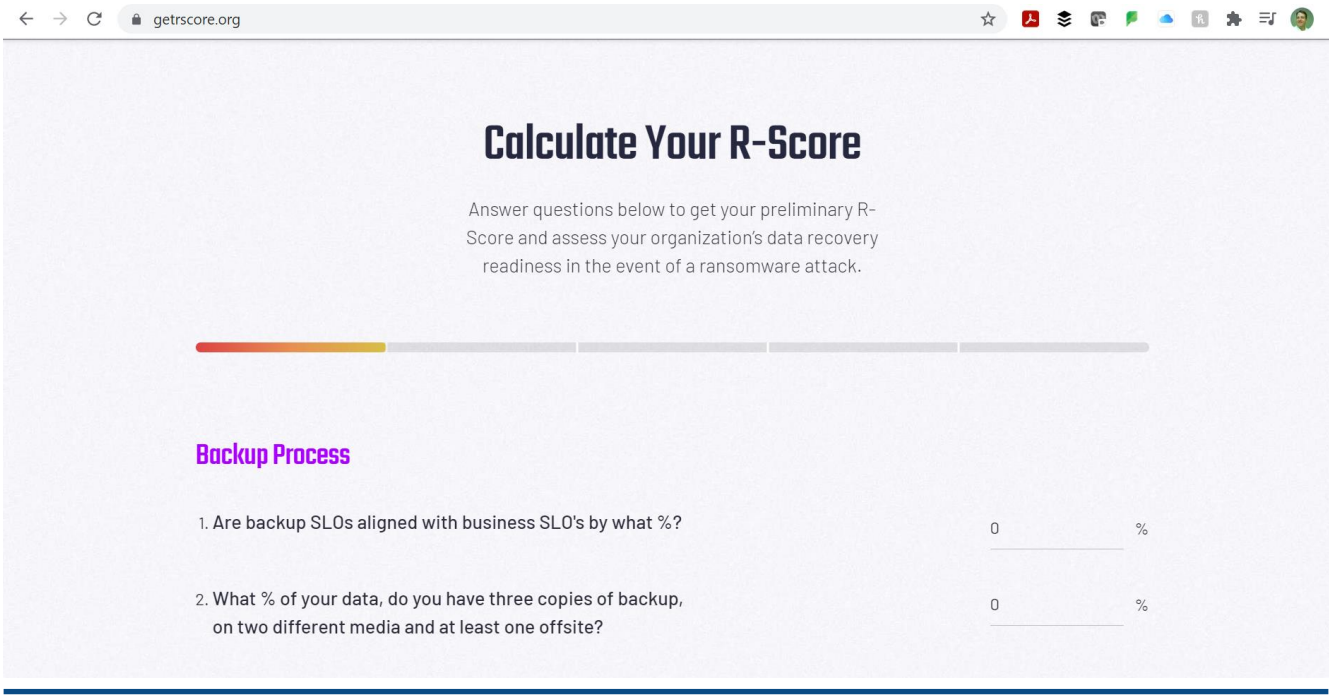

Figure 1 *Source:* HYCU

Security and Networking

There are only currently four questions in this section. The multi-factor authentication, segmented network, and implemented security measure questions were straightforward to answer.

The one question about the visibility of backup targets required us to understand how the survey defined 'visibility.' It primarily refers to any backup targets that are not easily accessible.

In the company, individuals define "visibility" and "easily accessible" differently. Some see any backup target connected to any network as being "visible" if it is not air gapped. Others define backup targets as being easily accessible only if they are visible over the Internet. We opted for the latter definition when answering this question.

Restore Process

This four-question section stood out for two reasons. First, we did not need to debate on any definitions. Second, two of the four questions failed to capture the restore capabilities of applications hosted in the company's cloud environment.

The company stores its cloud-based production data on cloud object storage with versioning turned on. This made it difficult to answer the two questions about the frequency of performing backup verifications and test restorations.

The company performs restores on an ad hoc basis for cloud applications as needed. However, these restores do not occur on any regular schedule as these questions asked. Further, the restores have, to date, always work when needed. While we selected the Ad-Hoc answer option for both questions, we felt we left some points on the table.

Disaster Recovery

The term "disaster recovery" sparked some dialog as the company feels it internally needs to redefine DR. For applications it hosts in the cloud, questions about hot and cold DR sites potentially become irrelevant. It configures all its cloud-based applications to run across multiple cloud regions.

This made it challenging to answer the questions about formal DR plans and frequency of DR testing. Its production cloud environment natively includes DR so the company never formally tests it. Conversely, we were unsure of the company's scope of DR preparations for its on-premises applications.

Due to the familiarity with the company's cloud implementation, we answered the questions in that context. The answers we choose reflected a more robust DR environment.

15 Minutes

We noted the time between when we started and completed the survey. Even accounting for the time spent discussing definitions and the company's environment, we finished the survey in fifteen minutes. We felt a single, knowledgeable individual might complete it even more quickly.

We've Been Warned

Clicking the Submit button at the end of the survey generated a final R-Score of 751. R-Score displayed the result in Yellow which we assumed was cautionary, and which HYCU confirmed.

R-Score also displayed the results for each section. Three of the five sections were green with the company getting dinged in the Security and Networking and Restoration Assurance sections.

Considering the company has, to date, successfully performed restores multiple times in the cloud, we downplayed that result. It probably scored low due to our uncertainty about the company's on-premises restore capabilities. We were also not super familiar

with all the intricacies of its networking and security operations so it is possible we left points on the table there as well.

Commendations and Recommendations

The final report shared the questions, our responses, and feedback generated based upon the responses. In areas where the company scored well, R-Score commended the company. For instance, it provided the following commentary:

- ***Using different media.*** Following the 3-2-1 backup rule indicates adherence to best practices which has less exposure to ransomware.
- ***Backup SaaS.*** SaaS offerings tend to be less complex while being more intelligent and robust.
- ***Using a public cloud for DR***. Businesses receive continuous access to highly automated, highly scalable, self-driven, off-site DR services.

It also provided recommendations for improvement. For example:

- ***Network segmentation.*** Consider creating segmentation in your backup network. This limits how far cybersecurity can spread by stopping harmful traffic.
- ***Data stored in an immutable format.*** All data not stored in an immutable format is still open to bad actors and may be impacted by ransomware.

HYCU R-Score Asks Questions Every Organization Must Answer

In completing this survey, we concluded the company scored reasonably well considering we lacked complete information. While not immune to a ransomware attack, it seemed to indicate a ransomware attack would not cripple the company either. We acknowledged its R-Score was likely skewed by our knowledge gaps and the need to make some judgment calls in the survey.

The survey's provided answers, scoring, and feedback did provide assurance about the company's ransomware recovery preparedness. However, we found the questions themselves provided the most value.

Simply knowing the right questions to ask should help organizations perform a baseline assessment of their ransomware recovery preparedness capabilities. They provide organizations a starting point for evaluating these components of their IT environment. They can then potentially develop their own answers and weightings and use their R-Score as a reference point.

In taking this survey, individuals may want to complete it separately for each type of environment protected. For instance, for applications and data hosted and protected on-premises, complete the survey in that context. Once completed for that environment, take the survey again and complete it again for the other IT environments in place, such as cloud, hybrid, and virtual.

Alternatively, individuals may also contact HYCU or its partners. They will freely provide a longer, more detailed survey so organizations may do a more thorough assessment.

Simple, Logical Starting Point

The R-Score survey provides a simple, logical starting point for organizations to quickly assess their ransomware recovery readiness. They get questions they can use, answers to ponder, and indicators on where potential vulnerabilities exist.

Perhaps equally important, organizations get answers to these questions and may put some plans in place. These steps minimally ensure organizations can respond to any third party should it questions them about their ransomware recovery readiness.

Whether organizations are ready or not, they should expect these types of questions to come their way. R-Score helps by positioning them to have some answers to these questions in potentially fifteen minutes or less. ■