Technical Insight Report

Evaluator Group Audit of R-Score™ – Ransomware Recovery

By Randy Kerns

January 2022

Evaluator Group

Enabling you to make the best technology decisions

Overview

R-Score™ is short for Ransomware Recoverability Readiness Score. It is a measurement system developed by HYCU and partners that assesses an organization's preparedness for recovering from ransomware using data from their data protection (backup and Disaster Recovery solution) software. The scoring looks at major aspects of recoverability in five areas and uses responses to a set of questions to create a "score" that reflects the ability to recover from a ransomware attack. Recovery from ransomware in this case is focused on returning to operation by restoring data that had been protected. In addition to being the basis for scoring, responses to questions are also used to provide recommendations and suggestions for improving readiness, resulting in an improved score.

Preparedness as represented by R-Score™ is about doing tasks and setting up the environment to enable the recovery of data. The resulting score is relative to individual improvements made on site and to participating organizations.

The **website version** of R-Score™ gives an initial rating of the readiness with a set of questions. This rating can be used for a simple comparative. A more comprehensive R-Score™ assessment dives deeper into the five areas and provides informative narratives on the questions and explanations regarding best practices for a particular area. This assessment is done with a HYCU Specialist or a certified partner in the area. HYCU developed the assessment tool and also provides an assessment engagement for IT personnel.

Evaluator Group Opinion

- The rigor for questions in topical areas and the complex scoring of responses accurately portrays recoverability readiness.
- Measures of the important elements for recovery were included in the readiness assessment.
- Assessment areas:
  - Backup Process
  - Backup Infrastructure
  - Security and Networking
  - Restore Process
  - Disaster Recovery Assurance

Evaluator Group was engaged by HYCU to do an audit of R-Score™, investigating the questions and scoring to determine whether the Ransomware Recoverability Readiness accurately reflects recoverability and has the integrity required to be an independent assessment without specific vendor promotion or skew. This paper is the result of detailed examination of questions and the scoring methodology with the background of expertise for recovery based on Evaluator Group's work with IT organizations in both strategy and actual recovery.

Audit Process

The audit process was an examination of the questions and the scoring based on responses. Understanding the questions and what an organization would typically do with the gauge of what best practices would entail comes from hard-earned experience. The following is a summary of items that were included for the audit. Additional investigation was done in areas when necessary.

- Do the five segments that are defined fit normal customer environments?
- Are the questions relevant to ransomware recovery?
  - Do the questions fit within the segmentation of the five that are defined?
  - Are they somewhat linear? (Would they be in a logical order in a discussion?)
  - Is there something missing that should be asked regarding ransomware recovery?
- Are the questions unambiguous?
- Are the questions self-serving for HYCU?
  - Leading to use of HYCU's solution?
  - Using terminology or phrasing specific to HYCU?
- Do the questions provide adequate information within each section to characterize the customer situation?
- Does the scoring really create a benchmark assessment?
  - Do the scores and weight for each question reflect importance for ransomware recovery?
  - Are the differences between scores for individual questions are proportional to the readiness difference?
  - Are the score choices comprehensive – applying value for each area of a particular section?

The goal from the review and subsequent investigation/analysis was to be able to render an opinion on the readiness assessment: Does it accurately reflect an organization's readiness from the score obtained? The claim then would be based on the rigor of the questions and a scoring system that reflects the importance of preparedness.

Each of the five segments covered a different area. They were evaluated by specific area to provide a more granular understanding of the impact to the overall score. The following sections are a narrative for each of the segments in the assessment that give Evaluator Group's comments on the questions and scoring.

Backup Process

The Backup Process section asks questions regarding practices for protecting data: whether the backups are completed in the time allotted as required for the business process, how the protection is done, how the protected data is secured, and controls around the backup process. The following are notes taken during the during the review regarding items of particular importance. Other necessary questions for understanding were investigated as well but no additional issues need to be brought up regarding the questions or the scoring.

- Reviewing the scoring for tier 1 data versus tier 2 data actions, the ratings are representative of the differences in value of the data. Various questions dealt with protection of the different types of data were asked.
- The type of snapshot and whether a snapshot is used is appropriately scored. Snapshots are additive to protection and not necessarily a penalty if not used.
- The 3-2-1 questions and scoring were done well – showing the importance of being consistent with a protection process.
- Scoring for what is air gapped for critical data highlights the importance for ransomware recovery. Knowing what data is critical is assumed and not included as a question.
- The importance of change control is often overlooked and the questions bring out the value.
- All questions were relevant and clear. Some were specific to ransomware recovery within the overall backup process.

Backup Infrastructure

The infrastructure for performing backup and recovery must be in place and resilient such that data protection and recovery can be done when needed and without interruption. In addition to the availability requirements, the infrastructure itself must have detection and preventative measures from attacks. The questions for this section bring out the protection solutions and infrastructure used.

- The ranking (and scoring) of the different backup solutions (SaaS, Appliance, software, snapshots) is appropriate given the complexity and risk details.
- The number of agents required to be installed on servers for protection is unlikely to be generally known and will require some research. This research, while it may take some time, will ultimately be valuable in characterizing the environment.
- Protecting the backup server/appliance is important and the scoring for this makes sense.
- Keeping the systems and software at the latest updated level is important for keeping security protections discovered by vendors current.
- Encryption of data at and during transfer is another security function that is applied at the infrastructure level. The importance and scoring represent the necessity. This is valuable for ransomware protection.

Security and Networking

Security is a critical area for protecting the backup data and infrastructure. With ransomware, the security area has gotten greater scrutiny and involves organizations and people outside the normal IT operations group. Networking is seen to be a vulnerable area for the security of backup data. Questions in this section cover multiple areas specific to security and have scoring appropriate to the heightened awareness of security practices required.

- Questions regarding credentials and multi-factor authentication show the importance of those security practices and have appropriate scoring.
- A relatively new requirement for many organizations is included regarding two person concurrence for low-level access to systems with backup data. This is an important question for ransomware and is scored accordingly.
- Certain industries have mandated using external key managers with the data at rest encryption. This is covered as well in the questions.
- Network segmentation and isolation for security is covered with questions in this section.
- Security of access to the backup data and visibility of the data falls into a number of areas and questions bring out the critical need for controls.
- A very interesting addition to the security area questions is in regards to the rigor of the vendors utilized for their security practices. Prior incidents have come from exploitation of vendor software so the questions in this area are important for ransomware protection.

Restore Process

The restore process covers the operations for restoring data from backups after an incident has occurred. Importantly, it covers the complexity of the restore process. This has been an inhibitor for many organizations because operations become more complex over time as new demands are added.

- During a restore process, especially where time is crucial, the need to set up environments such as when agents are required on servers before restores can begin. Appropriate questions are asked and scored that will cause some consideration of the complexity.
- Recover time is about the speed of recovery and can be for single sets of data all the way to complete environments. The questions ask about the different source for restores including snapshots.
- Validation of the data backed up to be recoverable is a key process. Questions about the process and frequency are covered and scored – demonstrating the importance.
- In addition to validation of the data, actual restore audits as if they were being done in earnest is a best practice that is included in the questions and scored appropriately.

Disaster Recovery Assurance

Recovering from a natural disaster seems to be happening with a greater frequency. Other disasters that are not weather related occur as well. This section deals with recovering from disasters with the expectation that a plan is in place with a 'run book' for the sequence of actions.

- An assessment of the plan for recovery is asked for and scored. For readiness assessment, this question is reflective for the individual but will be useful in understanding and seeing the impact on the scoring.
- Testing the Disaster Recovery Plan is necessary to know if it will work, find holes, and expose it to personnel that may not have taken part in the creation of the plan. The questions asked about testing the Disaster Recovery Plan and then scored show the value.
- Included questions about the Disaster Recovery Plan are regarding the target for recovery: to another site or a public cloud. These questions are really about the agility to adapt to different circumstances and are brought out in the scoring.
- As noted earlier, recovery time is an important factor for operations to be able to give to the organization. Questions in this area are about the time and necessity to set up the needed environment.

Ransomware Recovery

Ransomware recovery can be approached as disaster event and use similar procedure to traditional Disaster Recovery. The comments on Disaster Recovery Assurance apply for Ransomware Recovery with some additional actions.

- The selection of which protected copy to recover is an added factor for the recovery.
- Some ransomware recovery may require recovery of data to a sandbox to determine whether the data is free of infection. This capability is included in another question and the scoring shows the necessity of this capability.

Evaluator Group Rendered Opinion

The detailed examination of the questions and the scoring with the criteria cited earlier has validated the efficacy of R-Score™ Recoverability Readiness. Evaluator Group has confirmed the rigor used in the questions and scoring will accurately produce an indicator as a score that can be used as a relative measure. The final score is reflective of the accuracy in how the questions were answered. The comparative number will be useful in an assessment for IT organizations, first to create a baseline and then to gauge subsequent improvement.

Summary

The review of R-Score™ provided insight into a scoring system that, while complex, produced repeatable results that gave a measure for readiness to recover from an event. As with anything in IT, training and regular exercising of processes are required to be effective. But the measure, used as guide, will be very valuable for IT. The fact that this was developed by seasoned experts in a company that offers backup software has been proven to not favor the company product or the messaging. This truly is an independent evaluation of the readiness. Evaluator Group brought a healthy measure of skepticism to the project but, in final review, R-Score™ really does have the rigor and measures to accurately portray readiness to recover.

About Evaluator Group

Evaluator Group Inc., an Information management and data storage analyst firm, has been covering systems for over 20 years. Executives and IT Managers rely upon us to help make informed decisions to architect and purchase systems supporting their data management objectives. We surpass the current technology landscape by defining requirements and providing an in-depth knowledge of the products as well as the intricacies that dictate long-term successful strategies.