COMMVAULT

WHITEPAPER

Are you Ready? Intelligent Data Management as a foundation to operational readiness

By: Richard Breakiron | Director, Strategic Initiatives, Federal | Commvault
May 2021

Digital operational readiness

In a recent presentation to a NATO audience of cybersecurity experts, I opened with a simple question in big, bold letters: "Are You Ready?"

My question was not aimed at reaffirming the continual FUD thrown at us about cyber and ransomware events. Instead, it was meant to drive the point, "Do we really appreciate how dependent we are on our IT systems in our digitally transformed world?" The data that underlies today's modern business and mission operations is the lifeblood and when it stops flowing, our operations come to a halt.

The ability to be ready in a virtual world is significantly more difficult than operational readiness was before – and even before operational readiness was always a challenge.

The recent SolarWinds cyber disaster spread to its clients and it went undetected for months, not to mention the recent Honeywell breach and the Colonial Pipeline ransomware attack should have you thinking, "Wow, the cyber threat is getting serious, and it is now a matter of "when" and not "if"?"

If you are lucky, you were one of the organizations that realized 10 years ago the threat of cyber-attacks. Ideally, you have been building contingency planning throughout your business processes on your digital transformation journey.

However, if you feel that pit in your stomach or that little inner voice saying maybe we are not as prepared, keep reading. You can be empowered with positive and realistic steps to be operationally ready in today's digitally transformed world.

Ready your organization

The obvious: Successful restoration of operations requires advanced preparation – and not at the time an event occurs.

In a virtual world, this paradigm is even more critical. As an event is unfolding, the response time is measured in seconds, or if you are lucky, minutes.

The National Institute of Standards and Technology (NIST) Framework has Identify as its first of five steps which underlies 'advanced preparation'.

Focus on the critical. Get your team together and ask them key questions:

- What happens when we lose our network?
- What key operations must be protected with true 'fail safe' investment?
- What must be restored first if a major event occurs?

Work from business priorities and then bring in the technical team to see what interdependencies are identified. This approach recognizes that certain critical access points with IT systems impact multiple business operations.

Remember, "less is more" should be your guiding principle. Use prioritized planning to get rid of the non-essential data and information and processes. Look for ways that can be an automated process to manage the scale.

Steady your organization – Conduct fire drills

Creating confidence and improved response times requires testing your plans. Take the time to run a 'fire drill.'

Check your plan, test it. See what worked and what was left wanting.

Restoral plans need to be resilient enough to react to the next malware attack. Good plans that are not tested often fail. Confidence is built with actual practice as with any skill or process.

Your technical team is creating a recovery solution that is resilient across various failure situations. Designing recoverability across environments and providing automated and integrated tests of the procedures validate your recovery readiness state. Knowing the mission critical data and applications were already validated for recovery by an automated and tested process is that next step in enhancing the level of security, compliance, and operational readiness.

Respond and build on lessons learned

Did I mention that there will always be a next event? The adversary gets a vote and is always looking for a gap or weakness.

Intelligent data management requires integrated threat and anomaly detection to support security and business integrity, and operational preparedness. Integrated threat and anomaly detection, in this case, is an augmentation to the defense-in-depth approach – it is not meant to be a specific cyber sensor. Still, it works instead as a best business practice.

Recovery readiness is a core value for Commvault in designing and delivering its intelligent data management portfolio. Integrating required tools to measure the recovery readiness state continually allows rapid exposure of, and remediation of, problems, validates the recoverability of critical data and business applications through automated testing, and helps continually improve data security and reduce operational risk.

While backing up data has always been a core to recovery readiness, ransomware attacks now target these copies. Bad actors recognize that without holding the backup data hostage with the operational data, they lose their leverage.

Data backup copies must have a level of isolation that Commvault built into its code from its inception 25 years ago. With Commvault you can create copies that cannot be corrupted (aka immutable copies), create an 'air gap' with geographic and system separation from operational data, and leverage emerging cloud capabilities to enhance these solutions further while optimizing costs.

Providing data security while providing maximum flexibility for 'ease of administration' of software is a constant tension point in digital transformation. Securing data and providing protection for concerns such as privacy, theft, corruption, and deletion, whether by internal, external threats, either malicious or accidental, are critical elements of data readiness.

NIST Framework

A tool used to assess software solutions is the NIST Security Framework for Identify, Protect, Detect, Respond and Recover. This framework parallels much of the discussion and outlined steps above, which Commvault uses in its professional services engagements to help organizations improve their operational security and awareness of industry best practices.

An introduction to the functions
The five functions included in the Framework Core are:

1 **Identify**
2 **Protect**
3 **Detect**
4 **Respond**
5 **Recover**

Providing organizations the ability to integrate user identity, providing access with the least required privilege, safe from user error, with a complete granular logging and auditing capability with a simple and intuitive dashboard allows for rapid response and recovery.

Many data management issues begin with understanding your organization's internal operational procedures. With that understanding, potential security gaps and weaknesses associated with insider threats, compromised credentials, and sometimes human error can be identified.

Implementing control mechanisms that require two or more administrators (applying a 'four-eyes' principle) significantly reduces this category of threats and greatly improves operations. Using Machine Learning (ML) algorithms to detect anomalies in file activity, implementing unique 'target files' (aka honeypot files) allow an early warning about potential ransomware attacks, and having automated alerts sent directly to administrators further build operational readiness and risk reduction of intelligent data management systems to the entire enterprise.

A cybersecurity approach to maintaining a defense-in-depth strategy continues to be necessary but is no longer sufficient. This strategy must be coupled with a focused effort on operational recovery when those preventative measures may fail. Integrating intelligent data management provides the necessary added measures to mitigate the risk of our dependency on automation associated with the unrelenting digital transformation.

So let me ask you now, "Are You Ready?"

To learn more about Commvault's Intelligent Data Services, visit commvault.com/intelligent-data-services >

©1999-2021 Commvault Systems, Inc. All rights reserved. Commvault, Commvault and logo, the "C hexagon" logo, and "Be ready" are trademarks or registered trademarks of Commvault Systems, Inc. A complete list of trademarks owned by Commvault can be found here. All other third party brands, product names, and trademarks are the property of and used to identify the products or services of their respective owners. All specifications are subject to change without notice.