VERITAS

How Healthcare Provider Organizations Approach Business Continuity and Disaster Recovery.

Organizations must be confident in their business continuity and disaster recovery plan and ensure backup systems have the capacity to handle their data security needs.

Veritas Survey Findings Summary | January 2020

Contents

Introduction 3

Methods. 3

Findings 3

Commentary 5

Conclusion 7

INTRODUCTION

Whether faced with a natural disaster or a cybersecurity attack, health systems need disaster recovery plans to ensure that providers are able to care for patients without interruption and the latter's sensitive health information remains protected.

Organization size and type do not affect this need because patient care and security should always be a top priority. Protected health information (PHI) is particularly important to consider in these plans because the electronic health record can be vulnerable to ransomware attacks and insider data breaches. Such security threats compromise patients' safety and health information.

"The United States government defines hospitals as critical infrastructure because hospitals are necessary during even the worst disasters," claims Rick Bryant, national healthcare architect for Veritas.

Under the HIPAA Privacy and Security Rule, covered entities must have a backup of their data and contingency plan, which should include plans for data back up, disaster recovery and emergency mode operation. Having a reliable way to recover data and applications as well as proper security for sensitive information can ensure that a security incident does not jeopardize patient care.

Organizations must be confident in their business continuity and disaster recovery plan. One piece of this plan should include ensuring backup systems have the capacity to handle the needs of their data security.

Healthcare organizations are increasingly leveraging cloud-based backup systems as a low-cost, off-site backup option. The use of this solution and other disaster recovery strategies can vary based on the cost associated with data backup and security, the amount of data that needs to be protected and the resources available to an organization.

METHODS

Veritas commissioned Xtelligent Healthcare Media to conduct a survey to gain insight into various healthcare organizations' business continuity and disaster recovery plans. Between September 4 and October 4, 2019, Xtelligent sent electronic surveys to 81,580 individuals who self-reported working in a federal/state/municipal health agency, a hospital/medical center/multi-hospital system/IDN, an outpatient center or a skilled nursing facility. Those surveyed included individuals with job functions ranging from chief executive to senior IT manager and IT staff. Xtelligent received a total of 107 responses that were included in the analysis.

Those working in a hospital/medical center/multi-hospital system/IDN were the most likely to respond, but affiliations varied across respondents:

- Hospital/medical center/multi-hospital system/IDN: 48.6% (n=52)
- Skilled nursing facility: 37.4% (n=40)
- Federal/state/municipal health agency: 9.4% (n=10)
- Outpatient center: 4.7% (n=5)

FINDINGS

A majority of respondents in the four major categories noted above are confident in their organization's current business continuity and disaster recovery plan (see Figure 1).

Among all the survey respondents, 26 percent report being very confident in their organization's current business continuity and disaster recovery plan. Forty-six percent reported they were confident and only 4 percent reported not being confident with their organization's business continuity and disaster recovery plan.

A similar pattern emerged across organizational types. Among federal/state/municipal health agencies, 30 percent are very confident and 30 percent are confident. Those in hospitals/medical centers/multi-hospital systems/IDNs are 23 percent very confident and 48 percent confident. Skilled nursing facilities are 30 percent very confident and 50 percent confident while outpatient centers report being 20 percent confident and 20 percent very confident.

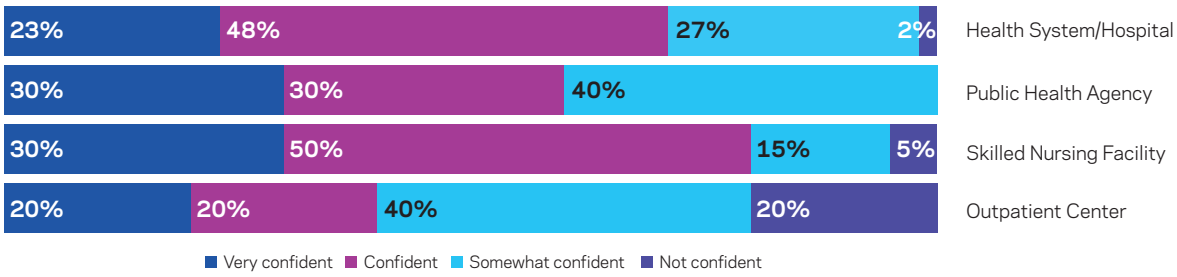

Figure 1. How confident are you in your organization's business continuity and disaster recovery plan?

Across all organization types, very few report being not confident in their organization's business continuity and disaster recovery plan: 20 percent, 5 percent and 2 percent of outpatient organizations, skilled nursing facilities and hospitals/medical centers/multi-hospital systems/IDNs respectively.

Hospitals are most likely to use a hybrid of on-site and off- site services for business continuity and disaster recovery (see Figure 2).

Respondents were asked the different methods their organization currently uses to handle business continuity and disaster recovery. Options included on site using tapes or other physical media, an off-site disaster recovery facility, off site using a cloud service provider, a hybrid solution or none of the above.

Hospitals/medical centers/multi-hospital systems/IDNs report using a hybrid solution 44 percent of the time, the most compared to all other organizations. Outpatient centers, skilled nursing facilities and federal/state/municipal health agencies report 40 percent, 33 percent and 40 percent use of hybrid solutions, respectively. "Hybrid solutions coupled with the legacy nature of many healthcare applications has caused increased complexity for recovering patient care services. This situation makes having an up-to-date plan and automation much more critical for effective disaster recovery," said Rick Bryant, national healthcare architect, Veritas.

Many organizations are still using physical backup disaster recovery strategies.

Thirty percent of federal/state/municipal health agencies report on-site backup recovery strategies and 10 percent off site in a disaster recovery facility. These organizations most heavily rely on physical backup recovery strategies because 13 percent of hospitals/medical centers/multi-hospital systems/IDNs, 8 percent of skilled nursing facilities and 0 percent of outpatient centers reported using on-site methods.

As Bryant explains, "Tape is a very cost-effective recovery method but comes at the cost of speed. In a critical industry such as healthcare, staying available and recovering rapidly can make the difference between life and death.

Cloud security is important to most survey respondents, but few are using this strategy (see Figure 3).

Organizations across the board agree that cloud security plays a vital role in their organization's recovery planning. Only 14 percent of all respondents said cloud security was not very or not at all important to their organization. Despite this finding, organizations infrequently report using an off-site, cloud service provider as a strategy for disaster recovery. Skilled nursing facilities are the highest users of off-site, cloud-based strategies (35 percent), while 20 percent of outpatient centers, 19 percent of hospitals/medical center/multi-hospital systems and 20 percent of federal/state/municipal health agencies report the same.

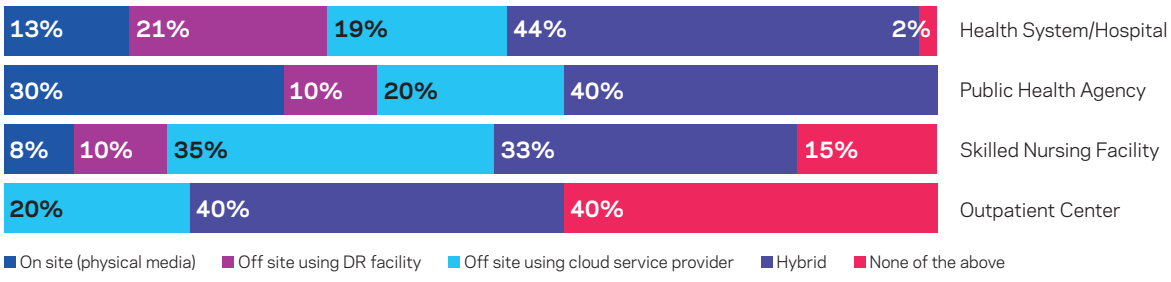

Figure 2. Where is your organization storing its critical data to ensure business continuity and disaster recovery?

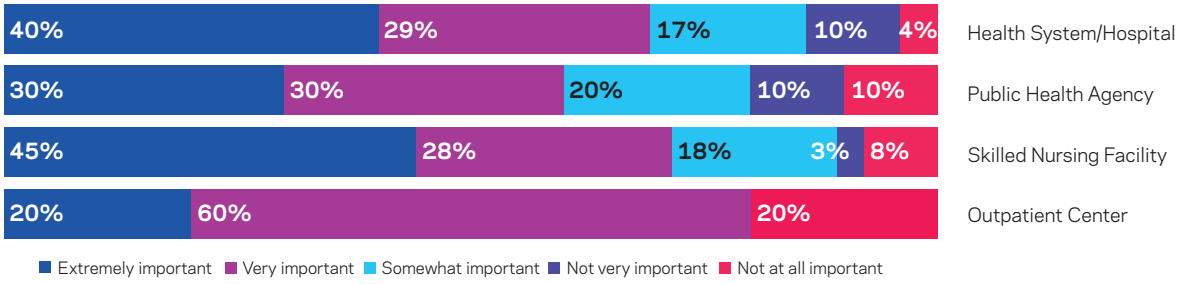

Figure 3. How important is cloud security to your organization's recovery planning?

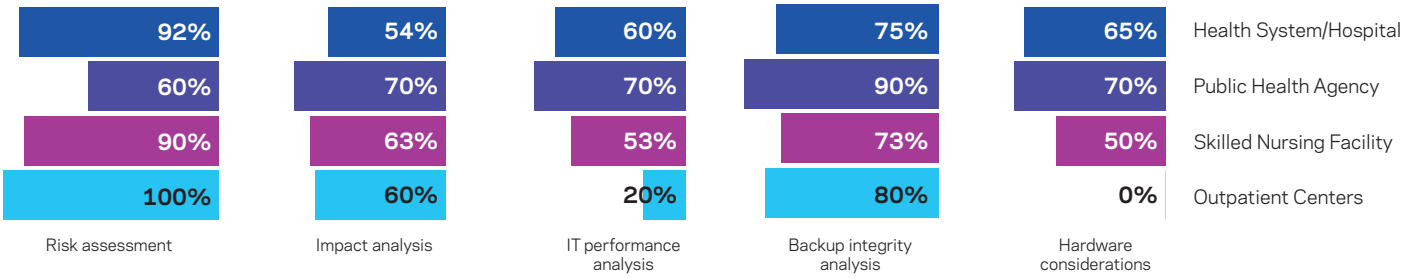

Figure 4. What factors does your organization consider in building its business continuity and disaster recovery plan?

Most organizations are using risk assessment, backup integrity analysis and impact analysis to build their business continuity and disaster recovery strategy (see Figure 4).

Risk assessments, backup integrity and impact analysis are the most frequently reported steps for organizations to begin building their business continuity and disaster recovery strategy; 89 percent, 76 percent and 59 percent of all respondents are using these strategies, respectively.

Results vary minimally by organization type, indicating that across the board, organizations understand the most important steps to building disaster recovery strategies.

To determine storage requirements, many organizations are deleting or archiving old data, varying storage types based on the importance of data.

For organizations to determine storage requirements for various data types, many report their strategy is to delete or archive data after a certain period of time. There is no consistency with the timeframe individuals report because it varies widely from three months to seven years.

Many others report stratifying the data by importance and the frequency of use. Old and unused data is then deleted or placed into less expensive storage options, and more critical data is stored on site, backed up or put into cloud storage.

Eight respondents report they do nothing to determine storage strategies, indicating that they do not have plans to cut costs for disaster recovery storage. Others say this business decision is the responsibility of someone else in the organization, such as the head of IT or an executive.

COMMENTARY

High levels of confidence in current business continuity and disaster recovery planning are at odds with the reality that many organizations still rely on physical on-site media as part of their strategy. Tape and disk, two forms of on-site physical media, pose security risks.

"Tapes tend to get lost. They are shipped off site, which means someone is responsible for their collection and transport. Anytime media is transported, there's an opportunity to lose it if they're not tagged properly. What's more, the vast majority of tape data is not encrypted," says Bryan Jenkins, director of sales at Carahsoft.

Meanwhile, a lack of encryption could expose physical disks to attack.

"Organizations tend to think that what's inside the perimeter is safe. And that's not the case. It's difficult to keep track of end users and their online habits. All it takes is a key logger or one right-click to get that code in-house. Disk is more secure than tape and a better alternative, but it has inherent risks."

On top of these vulnerabilities, tape presents additional limitations even when managed off site.

According to Jenkins, "Finding data on tapes is very, very difficult. Mislabeled tapes could lead to lost data. Also, tapes degrade over time when stored improperly. Tape initially looks appealing because the media is certainly cheap, but it gets costly at scale with petabytes of data."

"Unless data is encrypted, an organization is open to ransomware attacks. We see that more and more frequently as a result of phishing and social engineering. A bug gets inside, propagates and data is then held for ransom," Jenkins explains.

A hybrid of on-site and off-site services for business continuity and disaster recovery was the preferred method for hospital respondents. Still, the possibility remains that organizations are overspending on storage by backing up or maintaining redundant or unnecessary data.

"Organizations need to understand these risks before undertaking a serious backup overhaul, let alone moving to the cloud. Otherwise, they are throwing money out the door without a clear picture of what to store and manage," Jenkins warns.

"If an organization can cut down its backup environment by 50 percent or more, it can realize significant cost and time savings and a reduced risk posture. So, it's not just backup, it's getting a handle on the data prior to the backup. Once an organization knows what it is backing up, it is then able to back up smartly as opposed to offloading copious amounts of information into a data repository and hoping for the best."

Jenkins advises healthcare organizations to take advantage of assessment tools to find sensitive information within their data sets to detect the presence of PHI or personally identifiable information (PII). Stored improperly, this information could become compromised and expose HIPAA-covered entities to noncompliance and sizable monetary fines.

A useful mnemonic device is ROT—redundant, obsolete and trivial.

"Organizations can find ways to eliminate redundant data and reduce the amount of information to be backed up," Jenkins notes. "Obsolete data is past its shelf life, beyond the need for strict compliance. Additionally, trivial data has no reason to be backed up or managed. If organizations can address these types of data, they eliminate a sizable portion of waste."

High data availability is a requirement for healthcare organizations. A greater reliance on cloud-based business continuity and disaster recovery is no guarantee against data loss. "The downside to putting data in the cloud is that data still requires backing up. Cloud providers say data will always be available, but they don't necessarily say data will always be there," Jenkins acknowledges.

The solution to each of the risks mentioned earlier—storage, encryption and data loss—is effective testing of business continuity and disaster recovery plans. "An organization can buy all these high-availability solutions after realizing that its disaster recovery plan was not up to snuff. But a disaster recovery plan needs to be tested to make sure it works," adds Jenkins.

Tools to automate data restoration eliminate the headaches associated with typically manual processes.

"Most disaster recovery plans require multiple levels of approvals before any restoration takes place. Many of these activities still rely on manual processes," Jenkins continues. "And if an organization can't reach the database administrator to go and spin up all the databases and port them over to the other data center, it's stuck. Being able to automate that process and then test it regularly means that an organization can press a button and already have the approvals in place."

A business continuity and disaster recovery plan needs to undergo recurring scrutiny, and new technologies offer opportunities for refinement—from assessing data to be stored to streamlining the process of getting systems back online following a major event. To prevent out of sight from becoming out of mind, IT leaders must test their plans for effectiveness and implement new strategies to ensure that data access or lack thereof does not negatively impact clinical decision-making and patient outcomes.

CONCLUSION

Across the board, organizations report being confident in their business continuity and disaster recovery plan. Yet many are still using physical backups to manage their data, which leaves them vulnerable to natural disasters and physical security breaches.

Despite the universal agreement that the use of cloud-based backup systems is important to a disaster recovery strategy, few organizations report using this method. Leveraging this low-cost, low-maintenance technology can help healthcare organizations bolster their backup system and promote better disaster recovery strategies.

But healthcare organizations must still undertake regular testing of their business continuity and disaster recovery plans to gauge their effectiveness in ensuring the high availability of data in the event of a natural disaster or cyber threats. Restoring data from a backup can be a painful experience—one that healthcare organizations hope to avoid. In many ways, business continuity and disaster recovery investments are an insurance policy they hope never to use.

To safeguard their IT infrastructure against loss, corruption or a lack of availability, healthcare organizations should invest in technologies to manage the storage of sensitive and non-sensitive data, eliminate manual processes that slow data backup and restoration and test the effectiveness of their business continuity and disaster recovery strategies.

Produced by
xtelligent
HEALTHCARE MEDIA

ABOUT VERITAS

Veritas Technologies is a global leader in data protection and availability. Over 50,000 enterprises—including 99 of the Fortune 100—rely on us to abstract IT complexity and simplify data management. Veritas Enterprise Data Services Platform automates the protection and orchestrates the recovery of data everywhere it lives, ensures 24/7 availability of business-critical applications, and provides enterprises with the insights they need to comply with evolving data regulations. With a reputation for reliability at scale and a deployment model to fit any need, Veritas supports more than 500 data sources and over 150 storage targets, including 60 clouds. Learn more at www.veritas.com. Follow us on Twitter at @veritastechllc.

2625 Augustine Drive, Santa Clara, CA 95054
+1 (866) 837 4827
www.veritas.com

For specific country offices and contact numbers, please visit our website.
www.veritas.com/company/contact

VERITAS

V1002 3/20