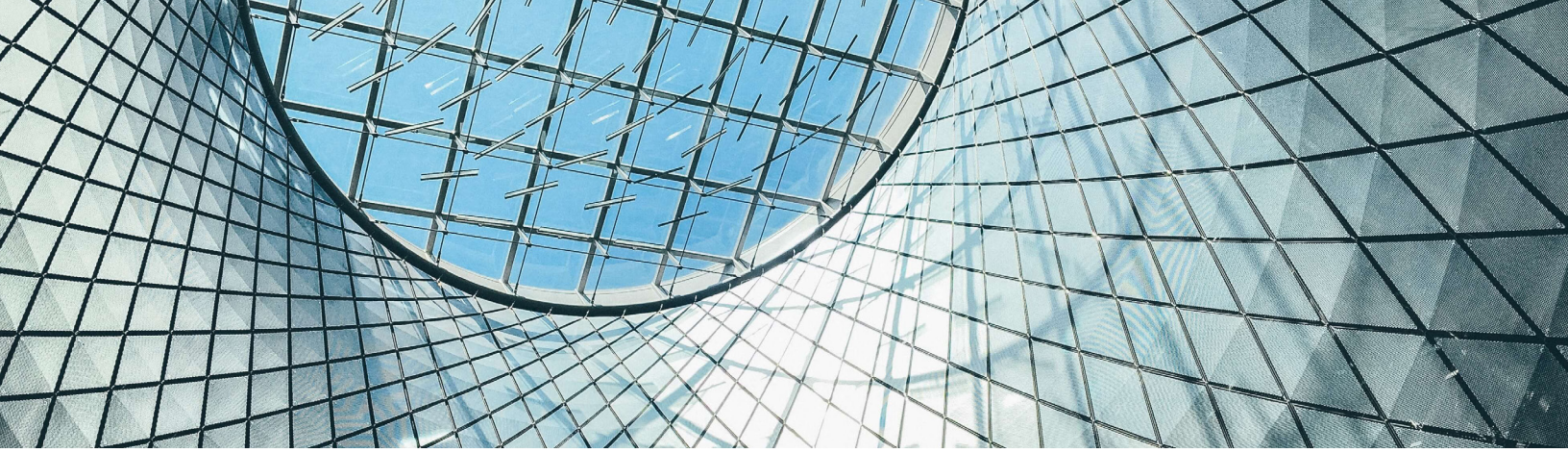


Market Insight Report Reprint

Many are confident they can recover from ransomware – is this justified?

August 31 2021

Henry Baltazar

The creation and storage of golden copies is a key process for recovering data that has been compromised by ransomware, but many organizations are looking to improve their recovery capabilities by storing multiple copies in multiple places both on-premises and in cloud storage services.

451 Research

S&P Global
Market Intelligence

Introduction

In our recent Voice of the Enterprise (VotE): Storage, Data Management and Disaster Recovery 2021 study, 62% of respondents had a high level of confidence (extremely confident or very confident) in their ability to recover their data after a ransomware incident. The creation and storage of golden copies is a key process for recovering data that has been compromised by ransomware, but many organizations are looking to improve their recovery capabilities by storing multiple copies in multiple places both on-premises and in cloud storage services.

THE 451 TAKE

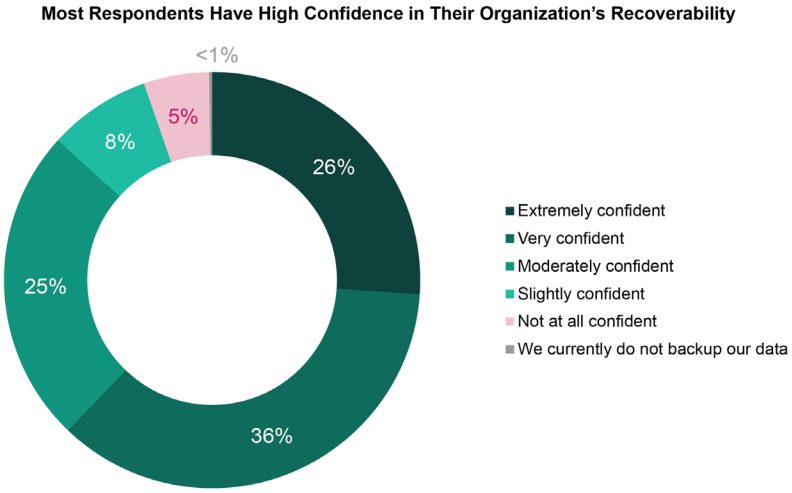
Ransomware has been a key concern for organizations in recent years, and in our VotE: Storage, Data Management and Disaster Recovery 2021 study, 73% of respondents claimed their organizations were increasing their spending on data protection as a result of the potential threat of ransomware. Backups and the golden copies that facilitate clean data restorations are the last line of defense when ransomware seizes control of an organization's infrastructure and cuts off access to data. The strategies on where and how these golden copies are stored are still up for debate. With service providers enhancing their ability to create and manage immutable storage, cloud storage is becoming a viable option for storing remote golden copies and providing customers with the benefits of elasticity and a remote recovery site.

Many end users would benefit from revamping their data protection and disaster recovery infrastructure by securing backup copies stored with a physical air gap or using immutable storage, and by adding proactive security tools to warn of potential ransomware incidents, such as suspicious file encryption activities. Organizations need to treat ransomware like other disasters, and ensure that runbooks and business continuity plans are in place and constantly tested to ensure they can facilitate a reliable and rapid recovery when the time comes. Although the majority of organizations in the study have taken steps to protect against ransomware, there is likely room for improvement, even though some have already pulled off successful recovery operations.

Backups and snapshots play a role in successful recoveries from ransomware

In our VotE study, 30% of respondents claimed that security issues such as viruses and ransomware played a part in their most recent outages. When asked about their ability to recover from ransomware, 26% were extremely confident that their current backup tools would facilitate a successful recovery, with an additional 36% saying they were very confident.

Figure 1: Organizations Are Confident in Their Ability to Recover From Ransomware



"Call it maybe 95% confident we could get it all back [recovering our data from backup after a ransomware incident]… There would be that last few hours or whatever between the time that it happened and the time we noticed it and the time we started recovering. We might leave a little bit of data there, but I'm pretty confident we would be able to recover effectively."

IT/engineering manager/staff
2,000-4,999 employees
$500m-$999.99m
Government

Source: 451 Research's Voice of the Enterprise: Storage, Data Management and Disaster Recovery 2021
Q: How confident are you of your organization's ability to recover data from a ransomware incident using its current backup tools?
Base: All respondents (n=452)

The quote above (Figure 1) from an IT manager working for a government entity encapsulates why many organizations are confident about their ability to recover, although we would note that, in this case, the customer was willing to accept data loss in the scale of hours to facilitate the recovery. Organizations that solely rely on daily backups for their ransomware protection do so with the expectation that any data created after the most recent backup could potentially be lost if an administrator has to restore a data volume back to the previous state. Another benefit of backup tools highlighted by this end user was that the Commvault data protection software the organization was using was warning the team about encryption operations that looked out of the ordinary during the daily backup scans.

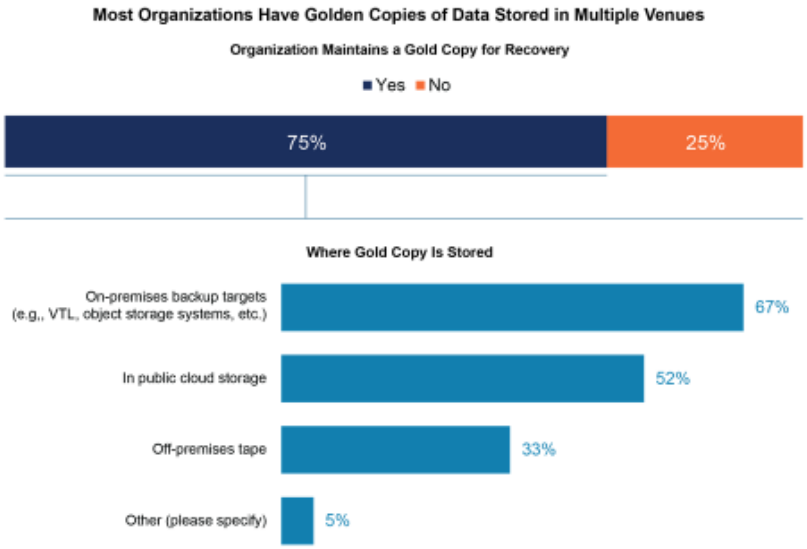
> "We had [several ransomware incidents a few years ago], and they've been nasty, but we recovered every single time…. The nice thing about having an enterprise-class NAS is that you have snapshots…[We] cut them off the network and then simply restored from the last setup. We lose a day…. So it's a bad day, but everybody thus far understands what's happened and they accept the cost."
>
> ––Healthcare IT/Engineering, Manager/Staff, Headcount 10,000-49,999, Revenue $5B-9.99B

In some cases, such as the Healthcare organization referenced in the above quote, the IT staff was able to leverage the snapshot capabilities of their Dell EMC Isilon NAS systems to recover from the incident, although that came with a day's worth of data loss. In an interview with a large retail organization, the IT staff further enhanced their data protection by using anti-ransomware tools from Superna to proactively monitor file shares on their Isilon NAS systems for suspicious activity and halt file synchronization operations when a threat is detected to prevent the spread. While snapshots, backups and replication are designed to protect data, if the data preserved in the backups or snapshots is already corrupted, then they will not facilitate a clean recovery.

Golden copies are an essential element for ransomware recovery

In our VotE study, 75% of respondents claimed their organization was already creating golden copies of data for the purpose of recovery from a potential ransomware incident. A golden copy is the official master version of a record of data, which organizations can refer to should the production copy of data become corrupted or destroyed. Although backups can provide a safety net in the event of ransomware or other disasters, organizations must ensure they are taking the proper steps to protect the golden copies they are relying on for recovery.

Figure 2: Golden Copies Provide a Safety Net Against Ransomware



"We haven't [had a ransomware attack]. And... one of the streams of the work we've got going on at the moment to consider how we protect ourselves from it... How do you have a third copy of your data somewhere that is safe and protected... A lot of our data backups are based on stuff being online... Do you need something purely offline and safer and completely segregated?"

Mid-level management
10,000-49,999 employees
$10bn+ revenue
Financial services

Source: 451 Research's Voice of the Enterprise: Storage, Data Management and Disaster Recovery 2021
Q: Does your organization maintain a golden copy of data to recover after a ransomware incident? (n=411)
Q: Where does your organization store its golden copy of data? Select all that apply (n=300).

In the backup world, the 3-2-1 rule is a well-known standard among storage professionals, calling for three copies of data (one production and two backup copies) stored on two different media types (e.g., disk, tape, cloud storage), with one copy stored in an off-site location. Backup vendors such as Veeam have also been pushing to raise the bar on these standards by suggesting that customers also make sure that one of their backup copies is in an offline and air-gapped format, such as tape, or in an immutable storage format in cloud storage or an on-premises object storage system that cannot be edited or deleted for a set retention period.

On-premises storage, cloud storage and even off-site tape are all potential places where golden copies can be stored, and respondents in the study were (on average) using two different options. On-premises backup targets were the most frequently used storage repository for golden copies in the study, and we believe this will continue to be a popular option because recovery from on-premises is likely the fastest option for a customer trying to restore data locally, since physical data transfer and transfer over WANs (for recoveries using cloud storage) are not needed. Public cloud storage will likely gain customers, as well, since many of the service providers now have object storage services with immutability capabilities to keep backups protected. Thirty-three percent (33%) of respondents are relying on tape to preserve their golden copies, and this method is still widely used despite the long restoration times associated with physically transporting tape back to a client for recovery.

CONTACTS

The Americas
+1 877 863 1306
market.intelligence@spglobal.com

Europe, Middle East & Africa
+44 20 7176 1234
market.intelligence@spglobal.com

Asia-Pacific
+852 2533 3565
market.intelligence@spglobal.com

www.spglobal.com/marketintelligence