Disaster recovery (DR) has long been important to business continuity.

IT professionals need to ensure that their data is secure and protected in case of an outage or serious catastrophe. While traditional DR has served IT pros with mixed results over the years, it has not evolved to meet the shifting needs of rapidly changing business climates.

This report provides the results of a survey of 343 IT professionals working across nine verticals, including healthcare, telecommunications, utilities and finance, and employed by companies ranging in size from under 100 employees to over 1,000 employees. The results are clear: traditional DR is broken. Protection has been degraded by insufficient resources, process complexity and competing IT priorities.
KEY FINDINGS

1. Respondents test their DR far too infrequently
With 58 percent of respondents indicating they test their DR just once a year or less, backup environments are at substantial risk in the event of an outage or disaster.

2. Lack of internal resources and process complexity are holding IT pros back
Lack of internal resources (56 percent) and process complexity (34 percent) are cited as the biggest reasons why respondents don’t test more frequently. It’s clear that traditional DR solutions are too cumbersome and difficult to manage.

3. IT Pros Want the Cloud
A stereotype persists that IT is overwhelmingly against the cloud due to perceived security and network concerns. However, 55 percent of respondents said they would embrace cloud DR as long as they could extend their on-premises network and security controls to the cloud. This suggests IT pros aren’t against the cloud, they just want equivalent controls in the cloud.

4. Recovery Point Objective lags in traditional DR
Recovery Point Objectives (RPOs) stand out as another compromise inherent with traditional DR. Only 21 percent of respondents said their RPO is less than 2 hours.

5. Oil and Gas Industry Woes
Responses were mostly consistent among all nine verticals, but IT pros from the oil and gas industry stood out with the greatest DR struggles. The industry had the highest average RPO (70 percent of respondents stated their RPO took 12 or more hours) and lowest testing frequency (80 percent of respondents saying they test just once a year or less). By comparison, for all industries, only 33 percent of respondents had an RPO of 12 or more hours and 58 percent of respondents tested once a year or less.
How Often Do You Test Your DR Environment?

- **Every Month**: 15.57%
- **Every Quarter**: 25.96%
- **Every Year**: 25.41%
- **Infrequently**: 26.23%
- **Never**: 6.83%

Infrequent testing was revealed as one of the *biggest issues* plaguing DR.

58 percent of respondents said they test their DR just *once per year or less*, while 33 percent of respondents said they tested *infrequently or never*.

Industry best practice suggests *testing at least once a quarter*.

Testing ensures a company’s DR solution is working properly. Without adequate testing, a minor datacenter outage could become a *serious headache*, and a major disaster could prove *catastrophic*. 
Why Don’t IT Pros Test More Frequently?

Lack of internal resources (56 percent) and process complexity (34 percent) are the two overwhelming causes for infrequent DR testing. The use of automation to deploy cloud DR can mitigate these issues, however. Automation expedites difficult manual processes and requires minimal oversight from IT staff.

The only organizations successfully employing traditional DR solutions are spending a large amount of money to do so. Due to cost and complexity, many other organizations have simply given up on delivering effective DR.

- DR vendor requires long lead time: 8%
- DR vendor charges expensive fees: 6%
- It’s too expensive to handle internally: 19%
- Not a priority: 29%
- Don’t have adequate IT resources to support testing: 56%
- Process is too complex: 34%
Embracing the Cloud

Conventional wisdom dictates that IT pros are weary of the cloud due to presumed security and network vulnerabilities. However, a majority of respondents (55 percent) indicated that they would embrace cloud DR as long as they could extend security and network controls to the cloud. This indicates that IT pros understand the clear benefits of the cloud and want to utilize it. However, it’s the process of moving not only their data, but their security posture, to the cloud that’s holding them back, not any overarching drawbacks of the cloud itself.

Advances in hybrid cloud automation now make it easier to migrate to the cloud.

Would you switch to cloud DR if you could automate network and security?

55% Yes
45% No
RPO is another area where traditional DR lags behind cloud DR, though the discrepancy isn’t as severe as it is in other metrics. Cloud DR can reliably reduce RPO to under one hour, depending on size and availability of bandwidth and the frequency the app environment changes.
### Secondary Data Center Failure and Delays

**When You Test Your Secondary Data Center, How Often Do You Experience Failure Or Delay?**

<table>
<thead>
<tr>
<th>Frequency</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>All The Time</td>
<td>1%</td>
</tr>
<tr>
<td>¾ Of The Time</td>
<td>8%</td>
</tr>
<tr>
<td>½ Of The Time</td>
<td>16%</td>
</tr>
<tr>
<td>¼ Of The Time</td>
<td>14%</td>
</tr>
<tr>
<td>&lt; ¼ Of The Time</td>
<td>61%</td>
</tr>
</tbody>
</table>

One in four respondents experience failure or delay over half the time when they test their secondary data center.
CAUSES OF FAILURE

What Are The Most Common Types Of Data Recovery Failures That Occur When Testing Your Secondary Environments?

*Network connectivity* was by far the most common cause for failure when testing a DR environment *(53 percent).*

*Wrong configuration* *(37 percent)* and *missing patches* *(33 percent)* were also cited.
A majority of respondents are able to get their DR environment up and running within 8 hours of an outage or test, but almost one third (28 percent) take over 8 hours. Such a gap would have a major impact on a business’s bottom line.
Respondents gave similar answers across all nine verticals included in the survey. However, IT pros in the oil and gas industry stood out from the group due to their challenges with DR.

The oil and gas industry has the highest average RPO, with 70 percent of respondents stating their RPO took 12 or more hours, including 30 percent who said it took more than 24 hours.

The oil and gas industry also tested DR the least frequently, with 80 percent of respondents saying that they test just once a year or less. The healthcare vertical tested the second least-frequently, with 69 percent testing once a year or less.

The consumer services and healthcare verticals were most willing to embrace cloud DR provided they could automate network and security controls to the cloud, with 65 percent of consumer services and 64 percent of healthcare respondents opting for cloud DR, given automation.
CONCLUSION

The time has come for hybrid cloud automation to support cloud migration and cloud disaster recovery (cloud DR) operating models.

With hybrid cloud automation existing IT teams can support disaster recovery with existing resources while enhancing protection and reducing overall costs.

To learn more about how cloud DR featuring automation can save you time and headache, visit www.cloudvelox.com