Getty Images

STORAGE > DISASTER RECOVERY

Your Disaster Recovery Plan Is Probably Out of Date

Disaster recovery plans can quickly become outdated, so many organizations need to modernize their approaches now and add more automation.

Karen D. Schwartz | Jul 24, 2020

As the head of disaster recovery and information security for a community bank, James Hinks thinks about disaster recovery a lot. Currently, he is spearheading the process of increasing automation and incorporating more cloud technology

"We are a community bank, so we have to stay up for our customers. That requires very high SLAs [service-level agreements], and in the case of an ev have a very responsive and robust disaster recovery setup," Hinks said.

To keep providing the level of service customers expect, Hinks' push to modernize the bank's approach to disaster recovery makes sense. And many other organizations are thinking along the same lines. For most, it's not a matter of whether you should revisit your disaster recovery plan and technology—it's a matter of when.

"With the growth of hybrid technology, business IT is evolving faster than ever before, and it really doesn't take very long for a DR plan to become outdated," said Steven Hill, a senior analyst at 451 Research, a division of S&P Global. "Systems, applications and personnel are always shifting, so a good plan needs to reflect those changes on a continuous basis, as well as adjusting to meet the evolving demands of data governance and industry compliance."

For most, a lot has probably changed since their original disaster recovery plan and technology were established. For one, the era of virtualization and the cloud has reduced the tolerance for outages to virtually zero. According to a recent study by Forrester Research and Disaster Recovery Journal, the driving reason for improving disaster recovery capabilities is staying online and competitive 24/7.

Another important factor is the pivot from a focus on component-level failure to a focus on service continuity. Instead of the traditional DR approach, which required a backup and recovery capability for each component, it's more about understanding your critical business services.

"You need to know the dependencies of those services to determine whether you are delivering the right level of resilience across the process," said Pete Renneker, managing director and U.S. leader of the technical resilience practice at Deloitte &

Renneker also pointed to the growing importance of cybersecurity recovery. While traditional DR focuses on maximizing the availability of systems, applications and data, the presence of malware in an environment that is highly replicated and redundant can cause real problems.

For years, the assumption was that if you have a disaster recovery setup in place, you should be able to recover from a cyber event. That's no longer true; the more critical a company's environment is, the more likely the company will use aggressive replication as its primary recovery capability. That, in turn, means the environment will be more negatively impacted from an event, not less.

"Companies have been thinking about DR as an availability-only challenge, but we see that an integrity-based event can weaponize the backup capability and ultimately take your systems down," Renneker said.

It's Getting Worse, Not Better

These new types of scenarios, such as little tolerance for downtime and increased cyberthreats, require a new approach. By thinking about technical resilience from a scenario planning perspective, you will be better able to prioritize by risk and impact. Focus on worst-case scenarios. These may be different for different organizations.

"What are the scenarios that you are most concerned about and how does your current program deliver a level of confidence in recovery or not?" Renneker said. "You can't just go from a traditional program focused on a single scenario overnight to a fully redundant resilient network that delivers an always-on experience. Think about how you need to shift your processes and procedures."

If most of your high-impact scenarios revolve around cyberthreats, for example

monitored and scanned for any potential changes to the data. While it's still possible for malware to enter the environment, this type of "cyber [illegible] access or destruction of data even if the malware delivers its payload, Renneker explained.

Once the event has ended and the DR team understands what was introduced into the environment, the team can carefully access the vault, pull the data into a clean room, cleanse it to a certified state and then recover back to your production network.

For many companies today, pressing scenarios probably focus on the work-at-home paradigm caused by the current COVID-19 pandemic. For example, many have moved toward technologies such as virtual desktop infrastructure (VDI) to enable employees to work from home. If that's new to the company, those VDI setups can introduce risk. If a VDI instance becomes a single point of failure, hundreds of employees wouldn't be able to work if the VDI infrastructure fails or experiences a server attack.

These things make it more important than ever to review all existing business and IT risks, said Naveen Chhabra, senior analyst for infrastructure and operations at Forrester. Every time they are reviewed, DR capabilities must be revised to be in line with the new risks or changed form and fashion of existing risks.

Hinks agreed, adding that managing disaster recovery is essentially technical risk management. "I have a plan where I have 'x' amount of dollars to mitigate risk to achieve the business's internal SLAs, RPOs [recovery point objectives] and RTOs."

Equally important to planning for the most important scenarios is keeping your disaster recovery and production environments in sync. Most businesses fail to do this, Chhabra noted.

sites are in sync, it will take much more time to recover, even if you are successful with your recovery."

Instead of syncing environments at the end of the month, Chhabra recommends doing so every time you make a significant change. "These mismatches are a constant source of problems," he added.

Automation can make a big difference in all of these scenarios. At the most basic level, the inherent automation capabilities of the hybrid cloud can really improve disaster responsiveness and adherence to policies. A hybrid cloud approach also enables orchestration. The latest generation of cloud-native applications and tools are typically designed to support automation, as well as provide for common, policy-based management that can span a number of cloud services.

Finally, automation is a big part of testing—something organizations simply don't do enough of. According to one report, 27% of organizations test their disaster recovery plans once a year or less.

Benefits of Frequent Testing

For First Mid Bank & Trust, testing is paramount.

"We place a large emphasis on DR testing, which we believe should run like a scheduled task where you are running different scenarios monthly or quarterly," Hinks said. "If you have a 100% success rate with DR testing, you aren't testing enough or across enough different scenarios."

Frequent testing is more important than ever, given the frequent changes businesses undergo.

earlier version, which may now be obsolete because of the way VM [illegible] implemented certain functions in its latest release. That makes validation critical.

As important as frequent testing is, it's also important to make sure that you are testing the right things. Traditionally, organizations have focused on testing applications, servers, storage arrays, etc. Today, it makes more sense to move away from component-level testing and toward testing interdependencies between applications.

"Move toward testing of the ecosystem: Maybe move from test networks to live network testing with multiple scenarios," Renneker recommended.

Finally, reassess who is involved in your disaster recovery planning and execution. It's a big mistake to focus only on IT or only on the business side. For example, your company may have an existing application or piece of infrastructure that is no longer supported but still critical to your environment. That's a risk, and requires planning a DR capability aligning to that risk. If you haven't planned either a migration or a recovery infrastructure for that legacy application or infrastructure, you are not aligning your DR investments to the business or IT risks. And if your recovery capabilities aren't aligned to that risk, you are probably either over-investing or under-investing, Chhabra noted.