PARTNER'S GUIDE TO
Providing a Complete Business Continuity Solution

There's one way to get to a soup-to-nuts solution for backup and recovery, disaster recovery or business continuity, and it's not just about technology. It's about sitting down with a customer and a blank sheet of paper.
By Scott Bekker

Too often between solution providers and customers, conversations start with a generalized need, move directly to a product, and proceed to terms and implementation schedules.

You could make a similar case for modern backup and recovery systems. Based heavily on virtualization technologies, the capabilities of backup and recovery products have similarly advanced over the old days when backup involved loading tape drives into a van.

It's an efficient way to do business—if a customer knows it wants something, and the solution provider represents a product, why complicate things? The answer with backup and recovery is that the issue is far too important to proceed based on assumptions. A customer might think its partner knows what it needs, and the partner might think the customer knows what

it's offering, but that's never the case without a thorough and open conversation.

The spec sheet of what a backup and recovery, disaster recovery or business continuity solution offers doesn't begin to cover the territory.

The only way to build a comprehensive backup and recovery solution for a customer that covers disaster recovery and business continuity is to sit down with a blank sheet of paper, or a blinking cursor on a laptop, and start working through some important questions. Some of them are old chestnuts that still need to be talked over. Others are emerging due to recent trends, especially the proliferation of free or low-cost cloud services.

WHAT ARE THE CROWN JEWELS?

This is the absolute, critical piece to understand. Knowing which applications run the business, where they store their data, how frequently those applications are writing new data and so on is the centerpiece of any business continuity strategy. The crown jewels should be a relatively short list of applications, and this is where the most thought, resources, effort and expense of the business continuity strategy should be concentrated. These are the applications that must adhere to iron laws of backup, like the 3-2-1 rule—three copies, two types of media and one copy off-site. In fact, the crown jewels should probably be 3-2-2, with the second off-site copy at a geographically separate location from the first.

WHAT ELSE MATTERS?

Keeping the crown jewels list short means you'll need another list of important applications to back up. These applications might be the Exchange server or the SharePoint server—critical, sure, but able to be down a little longer without catastrophic results.

WHAT WOULD HAPPEN IF YOU LOST IT?

Once the crown jewels and the next tier are defined, the next question is what would happen to the business if the data was lost. Would the customer be able

to recover vital business records from paper copies, for example, depending on the type of business? For that matter, this question might lead to a discussion about adequately protecting paper records on-site from fires or floods. Assessing what would happen to the business if the data was permanently lost is foundational in determining how robust a solution a customer will really need.

WHAT'S THE ABSOLUTE LONGEST YOU CAN WAIT TO GET IT ALL BACK?

In nearly every business, there's an amount of time that would pass without its data where it would become extremely difficult, or require drastic measures like furloughs and layoffs, to stay in business. Knowing that time frame, which might range from hours in rare cases to days to weeks, is important in crafting a complete solution.

HOW DIRE OF A SITUATION DO YOU WANT TO PLAN FOR?

It's important to understand what types of problems are likely in a geographical location and for how severe a problem the customer really wants to be ready. Not everyone needs a regionally redundant recovery scenario. A business that has primarily local customers might not want to spend the money to maintain

> Assessing what would happen to the business if the data was permanently lost is foundational in determining how robust a solution a customer will really need.

uptime in a regional catastrophe, such as a Category 5 hurricane, if it knows its entire customer base is going to be evacuated and cleaning up themselves.

HOW COMFORTABLE ARE YOU WITH THE CLOUD?

Some customers see the value in cloud technologies and the way the cloud can give them extremely robust, enterprise-class solutions for small to midsize business and midmarket prices. Others still don't trust the idea that their data is going to be under the control of an entity with which they don't have a direct, personal relationship.

WHAT DATA IS ON THE LAPTOPS AND DESKTOPS?

Backing up SharePoint and file servers is great if that's where the files are stored. Yet users at many organizations keep important documents on their laptops. Understanding a customer's institutional culture and the work style of its employees is critical to making sure that the organization's most important documents

are backed up. It's vital to combine the answer to this question with the earlier question, "What else matters?" If it turns out that business-critical data is spread throughout the organization on laptops, desktops, tablets and smartphones, those devices had better be part of the business continuity plan.

ARE THERE MULTIPLE OFFICES OR HOME OFFICES?

A multi-office environment both complicates things and creates options. For one thing, having multiple locations often means additional servers to backup and recover. But having several offices presents an opportunity to provide redundant locations for backups without going outside company property. As for home offices, those are less likely to have servers to back up, but more likely to have users who keep all of their work on a PC or laptop and rarely or never store them on backed up file servers.

DO END USERS ADHERE TO THE BACKUP POLICY?

There are a few a buried assumptions in this question—that there's a clearly stated backup policy for the organization, and that employees are aware of it. The policy is a good place to educate employees about where they are expected to store company files, how often they can expect those files to be backed up, and what processes to go through to recover older versions of files, if that's an option. No matter what's in it, having a backup policy for end users is a best practice in any business continuity plan.

HOW GRANULAR DO YOU WANT THE RECOVERY CHAIN TO BE?

There are two ways to look at this question. Some backup and recovery systems can allow for individual e-mails to be restored or for previous versions of files to be recovered. So that's granularity in terms of documents and e-mails. The other way of looking at it relates to how many minutes or hours of data an organization can afford to lose. That answer determines the frequency of incremental backups on the crown jewel applications and the others.

WHAT'S IN THE ENVIRONMENT?

Another question that will determine the technological approach is to figure out what platforms need to be backed up. The servers might be all Windows in some cases, or involve numerous Linux distributions in others. Are there Macs or Chromebooks in addition to Windows desktops? Check that versions line up with the OS versions supported by the backup and recovery software.

WHAT CLOUD SERVICES DOES THE COMPANY OFFICIALLY USE?

The infrastructure that businesses use to run their operations is no longer exclusively under their control. Companies from small businesses to multinational enterprises have many of their

applications in the cloud via Software as a Service (SaaS) and files in the cloud via cloud storage applications, such as Dropbox or OneDrive. For one thing, it's a good idea to check the answers to this question against the company's backup and storage policy. Do they want to allow employees to store files in Dropbox, for example, rather than on the corporate file server? For another, this question opens up a discussion about whether the company should be trying to back up cloud service files separately or leaving it to the cloud services provider/SaaS provider to handle it.

WHAT CLOUD SERVICES DON'T YOU KNOW ABOUT?

You can't get an answer to this one from a discussion with top executives of a company, but it's worth helping them put out a brief employee survey to find out. Vendor surveys have found hundreds to thousands of cloud services at use in companies, with corporate managers often clueless about in which ones employees are keeping company data. By helping a customer quantify employee cloud usage, you can also integrate the knowledge into the backup policy, if necessary, and integrate the applications into the overall business continuity plan.

WHEN IS THE BACKUP WINDOW?

Advances in backup technology mean the backup disruption ranges from non-existent to a fraction of the load the process once put on corporate networks. Nonetheless, it's important to understand the rhythm of the business in order to schedule backups at the right times.

WHAT'S OUR RECOVERY TEST SCHEDULE?

The more frequently customers and their solution provider partners test the recovery of a system, the more likely the system is to work in a real emergency. Confirming that a given backup

job completes is important, but not nearly enough. Every so often there needs to be a full test involving recovering various systems on different hardware and making sure the recovery copy is fully operational. Use the customer conversation to agree on a regular schedule—quarterly is a good starting point for the discussion. Systems and priorities change faster than anyone expects.

HOW OFTEN DO WE WANT TO REVIEW THE WHOLE PROCESS?

One other important follow-up is to schedule the next time the solution provider and the customer should review all of these questions. Annually or every other year, it's a good idea to get back together and make sure all the earlier assumptions are still working and that all critical systems are covered.

These 16 questions provide a good start—every partner will develop a few of their own that lead to insights for both parties. The conversation prompted by these questions gives you a great chance to develop a comprehensive plan that meets the customer's needs within the customer's budget.

And the side benefit? To be of real value, a business continuity conversation has to be extremely wide-ranging. Insights you gain about the customer's business can lead to other IT projects and opportunities in dozens of areas. •

Scott Bekker is editor in chief of RCP *magazine He's been covering storage, backup and recovery technologies for nearly two decades.*

Backup Strategy Questions

What are the crown jewels?
What else matters?
What would happen if you lost it?
What's the absolute longest you can wait to get it all back?
How dire of a situation do you want to plan for?
How comfortable are you with the cloud?
What data is on the laptops and desktops?
Are there multiple offices or home offices?
Do end users adhere to the backup policy?
How granular do you want the recovery chain to be?
What's in the environment?
What cloud services does the company officially use?
What cloud services don't you know about?
When is the backup window?
What's our recovery test schedule?
How often do we want to review the whole process?

UNCOMFORTABLE

COMFORTABLE

Having your feet to the flames because of an IT disaster is a quick way to lose time, money, and your reputation. The last thing you want is a painful trial by fire. But using the StorageCraft® Recovery Solution,™ you'll know you can quickly, easily recover from any type of disaster. With trouble miles from your mind, "feet to the flames" will really mean fuzzy socks and hot cocoa. How's that for comfort?

Follow the link, or scan the QR code to see how
StorageCraft helps make MSPs feel all warm and fuzzy.
www.StorageCraft.com/warmandfuzzy

STORAGECRAFT®
RECOVERY
SOLUTION™