STORAGECRAFT.
RECOVER-ABILITY™
GUIDES

Making IT Disaster Recovery Easy

How asking questions can strengthen your disaster plan and save your business

By Guy Baroan and Casey Morgan

It's easy these days to back up your IT environment. Modern, image-based backup software makes it possible for you to protect your entire system by making copies of your data, your OS, your settings, and so on. You can even replicate those images easily to the cloud for extra protection.

What's not so simple is making sure you can always *use* that backed-up data. IT environments can be so complicated in today's businesses that even if you're using a great disaster recovery solution, recovery can be a real challenge. So what can you do to make any recovery easy?

Plan ahead.

When you consider your backup and disaster recovery plan, think about how it integrates with your business's overall IT environment and how together, they can create solid business continuity.

Consider what you need to know ahead of time in order to guarantee recovery. What do you need for a site-wide catastrophe that you don't need for a low-level server failure? How do you determine which pieces of equipment are most important?

You need to know everything there is to know about the environment you're trying to protect and you may not have the answers you need right at the start. But it's up to you to find out.

In this ebook, we suggest a number of things we think you should look at. The depth of evaluation may seem daunting, but if you take a little extra time at the beginning, you'll save tons of time and money in the end.

Let's get started.

Document Everything

Our first suggestion is simple: document everything.

As you evaluate your IT environment in preparation for a potential disaster, write everything down. Don't skimp on the details. Start with as much information as you can. You can winnow it down later.

If you plan on protecting (or saving) your business, you need to figure out what it has and what it needs. Whether you're making a plan for the first time or reviewing one that's already in place, the most basic thing you can do is understand what you're working with, from equipment to connections to services and so on.

After all, how can you possibly protect your business's IT without knowing what you're supposed to protect? For all you know, you may need all new equipment. Or maybe you may have a few pieces of good equipment you can build on. Either way, you need to assess everything.

Of course, "everything" is a daunting word. Ultimately, you'll have to decide how much detail you go into based on your time and your other responsibilities. Just keep in mind that the more comprehensive your assessment, the smoother your recovery will be.

Basic Information

A good way to start is by gathering information on all the key stake holders within your organization for a disaster. Who knows how to do what? Who needs to know immediately what's going on? Who has the keys? Who has access to the passwords? Etc.

The utility of some of these details will change from disaster to disaster. Your CEO probably doesn't need to know every time an employee's laptop breaks, but in any disaster (especially a big one), it's vital to have clear communication. Gathering contact information for everyone involved in one place, along with an idea of who's going to do what and who needs to be involved, makes sure no one's scrambling when the time comes.

Equipment Inventory

It's also helpful in the beginning to gather a simple survey of all your equipment. In a bit, you're going to be gathering a lot of detailed information about each piece of hardware, so by starting with an overview, you're making it easier to keep track of what you've already gathered and what you still need. In your list, you'll also want to include at least a general location for each piece of hardware, including those listed here (if applicable):

- Servers
- Desktops
- Printers and copiers
- Laptops
- Wired telephones
- Projectors
- Speakers and sound systems
- External hard drives
- Networking equipment
- Extra equipment, including keyboards, mice, and other peripherals (it never hurts to know what's available)
- Tablets and smart phones (see "Working with BYOD" in the sidebar)

Working with BYOD

Whether you support them or not, it's useful to understand which employees have tablets and smart phones.

In an emergency, employees can rely on these to communicate or, to a certain extent, to work when workstations aren't available. You may choose not to support employees' personal tablets and mobile phones, but it's helpful to understand what's out there.

Employee-owned devices can have a significant impact on a recovery, both positively or negatively. By keeping track of BYOD activity in your company, you can make sure that you're accounting for it when you make your plan.

Once you've got this general information about your environment, it's time to start digging in, a process we call the "discovery phase."

Equipment

First, start fleshing out the inventory you've created. Obviously, some equipment is more important than others and some information won't be relevant for every piece of equipment, but start by gathering as much of the following information as you can for each piece of equipment on your inventory:

- Equipment type (PC workstation, server, router, etc.)
- Serial number
- Model number
- Other identifying numbers you may use
- Age
- Warranty information
- Manufacturer name and customer service phone number
- Backup configurations (if they're in place)
- Primary and secondary (if applicable) purposes of the machine
- Disk partition size
- IP address or addresses
- SSID numbers for wireless routers
- Software, versions, and license numbers on the machine
- Name of user (especially for employee workstations)

Credentials, Access, and Utilities

Next you need admin rights and credentials, and with them, you need to know how routers and switches are connected. These are essential, since not being able to connect them means the pieces of the network can't communicate. With that in mind, find a secure way to record the following information:

- Email and web-host control panel credentials
- Cloud computing credentials (web-based applications and things of that nature)
- CRM, CMS, or other necessary software credentials
- Firewall configurations
- Domain admin credentials
- Router, firewall, switch, and other critical local usernames and passwords
- Internal IP addresses and DNS settings for servers, routers, and switches
- External IP addresses, remote domain names, remote web workplace logon credentials
- Notes on router port-forwarding
- VPN details

Once you have that, you're pretty close to a first draft. But remember, you also need to take into account things that aren't IT related.

Gathering Information

Gathering information can be done manually, but it's also useful to use remote monitoring and management (RMM) tools to keep you from needing to access each piece of equipment individually. A mixture of remote and manual information gathering may work well too.

For example, the techs at Baroan Technologies manually gather serial numbers and model numbers. But they also use a software collection tool. Once they've installed their agents, the program goes in and gathers detailed information about the hardware and the software versions.

Leaning on RMM tools can save you a lot of time, since agents gather information remotely and can document most of what you need automatically. If you aren't already using them, think about whether implementing RMM technology is a worthwhile investment.

How are you getting power, telephone, and Internet service, and who is your domain provider?

It's also important to look at contact information and account numbers for public service and Internet providers, not just equipment. You never know which service provider you might need to call in an emergency, so again, get everything. For example, write down the following information:

- Telephone provider phone number and website
- Internet or cable provider phone number and website
- Domain registrar and account information
- DNS provider or other third party hosting phone numbers and websites
- Public domain name information
- Power company phone number and website
- Account numbers for each of the above

Diagrams and Essentials

Once you have the above information, you also need network maps in order to properly visualize how everything works together.

This allows you to identify equipment dependencies, how network switches, routers, and firewalls are set up, and so forth. You don't want to wonder how the network is functioning. You need to be able to look at a map and see how the whole thing fits together with a simple glance.

Using a visualization program like Visio, diagram everything. If at all possible, write corresponding IP addresses, credentials, and necessary information next to each piece of equipment on the map. That way, you can visually see which information goes with which piece of equipment.

But that's not all. Knowing what something looks like in real life is much different than what you see in a diagram. The solution? Just like backing up a system, you need to take a snapshot. Take a photograph of each machine so anyone using the map will be able to identify anything.

Once you have your map, you're ready to start analyzing your IT environment in order to get a comprehensive plan ready.

Analysis lets you determine what your upgrade needs could be, what sort of equipment dependencies are there, and what you might be able to limp by without.

Some of the following might be questions to explore as you look through the information you've already gathered. Remember that the point of all of this is not simply to have information about your environment, but to use that information to ensure your environment is as efficient and disaster-proof as possible.

Take the time to identify the following:

- Which pieces of equipment could be upgraded or are near the end of their life and thus at a higher risk for failure?
- Which equipment is most essential? Can you get by without a file server? What about an Exchange server?
- Which of the essential equipment can tolerate downtime? How much downtime? An hour? A day?
- What is the monetary cost of downtime if the whole business is down?
- What is the monetary cost of downtime for individual pieces of equipment?
- What are the dependency chains, i.e., what equipment requires what other equipment to function properly? This is especially important for essential machines.
- What's missing in the network? Is everything set up efficiently? Is there a better way to set it up?
- What redundancies already exist? What redundancies can be added?
- What could be done to improve this network? Are there opportunities for cloud-based computing that might help cut costs? What about virtualization? How will those things affect the backup and disaster recovery plan?

Copying Your Documentation

I know how important documentation is, but during Hurricane Sandy, I couldn't access the information my team had worked so hard to gather.

A lot of people take for granted that they've got everything at their fingertips. They think they can use Dropbox or Evernote and have a copy offsite or anywhere you can think of.

Then they have a blackout and can't get anything.

Consider having a printed copy that's reviewed at least once a week, depending on how complicated the business is or how often you change things, and then update it as necessary.

And make backup copies of your printed versions. Have one copy in the office securely locked in a file cabinet or safe and one offsite at the your home. You need a physical copy of everything.

—Guy

Share the Goods

Chances are, you're not the only one who has a stake in your business's disaster recovery plan.

More often, executives, managers, and other members of your team have an interest in making sure things run smoothly, not to mention insights on non-IT considerations that you may not be aware of. And unfortunely, sometimes you may need to justify the cost of a disaster recovery plan.

The next step, then, is to share what you found in your discovery.

Once you've shared your documentation, these other members of your company will have an easier time understanding what's going on. This contributes to better IT decision-making and reveals the real value of a backup and disaster recovery plan. By painting a clear picture of the business's existing IT environment and by showing how everything's connected, you're helping the other members of your company see the positive ROI the company will get from implementing a disaster recovery solution.

Using your documentation, it's time to make some recommendations. Discuss current company objectives and make suggestions on how better recovery times can contribute to those objectives.

Then, use what you've found to explain how to achieve those better recovery times. Since you've gone through the exhaustive process of exploring the entire business, you're in a perfect position to discuss holes you can fill.

Discuss Goals

As you talk about infrastructure, it's time to gather a different kind of inventory.

You can't act on what you've learned during the discovery phase until you understand your company goals and expectations. This allows you to see how everything works together in a different way.

At this stage, consider discussing questions like the following:

- Do we have a backup and disaster recovery plan already in place?
- Do we have current recovery time and recovery point objectives (RTO and RPO)?
- Do we want to improve those RTOs and RPOs?
- Do we understand which pieces of equipment are most important to our business?
- Do we have plans for upgrading our equipment?

You may not know the answers to these questions and that's okay. Part of what you're doing in this step is discovering how much education other stakeholders in the company need. Be prepared to offer your own recommendations along the way.

One way to do this is to phrase your questions in terms of scenarios:

1. What if we come in tomorrow morning and our main server is completely down?
2. How long can our business operate without it?
3. How productive can our employees be without it?
4. What if all our servers were down?

Once you understand the company's objectives and needs, you can really start working backwards and say, "here's what you have and here's where we need to go."

And once you understand the business's tolerance for downtime and its other needs, you can start making your plan.

Talking about Cost

Having 100 percent uptime is expensive, but the truth is that you may not *need* it. It's important to carefully analyze your tolerance for downtime in order to determine a cost-effective solution. That way, you're not paying for something you don't need.

Of course, everybody *wants* 100 percent uptime, at least until you explain the cost. Walk through your company's real needs and look for situations and setups where downtime may be acceptable. If your business really has zero tolerance for downtime, the cost will be much higher, but if it can tolerate an hour or two, then it will be much less.

You've written down most of what you need and talked to others in your company, but the toughest part is yet to come.

Based on the information you've gathered on both your company's goals and your IT environment, it's time to set up a system that will function after minor hiccups or dire failures. This process involves creating redundancies, reducing dependencies, and turning the information you've gathered into a successful backup and disaster recovery plan.

Backup Configuration

After you've looked at which pieces of equipment you have, you need to decide which pieces will be backed up and where those backups will go. As with the discovery phase, setting up a good backup starts with asking some questions.

Does you have network attached storage for backups? A BDR appliance? A RAID array? Are you taking backups remotely using a management console or do you expect employees to be taking backups? Will backups be kept locally, offsite, or both?

If you're going to send backups to the cloud, how easily can you get to them? Does your cloud vendor allow you to virtualize a backup image in the cloud for quick failover? Do you have to call the vendor to virtualize or can you do it yourself at a moment's notice?

As you answer these (and probably other) questions, you'll be able to set up backups that meet the your needs. Once you've established backup configurations, be sure to make them clear on the network maps you've created.

Equipment

The goal here is to create a disaster recovery plan that will be as effective for one kind of disaster as it is for any other. The best way to do this is to create redundancies that eliminate dependency. The first place you'll want to do this is with equipment.

You already know where your backups are being stored, but those backups will be useless without equipment for the images to run on. Look at your equipment list and make note of how many extras (if any) you have of the following equipment:

- Network switches and routers
- Failover-ready equipment
- Employee workstations
- Cell phones
- Printers
- Cables

You'll need to fill in the holes as best as you can. The more extra equipment you have during a disaster, the easier time you'll have recovering (assuming it's the right equipment). You'll also want to think about where you'll get more equipment if you need it during a small failure, a large emergency, and anything in between. Many hardware vendors have options for shipping new hardware quickly, so consider asking what options are available before you need them.

If there's a large enough disaster, planning for hardware and software failure might not be enough.

Your IT environment is dependent on plenty of things outside the scope of your technology itself.

Site

For example, what if you can't continue working from your office? Work with your facilities team (or whoever handles building issues in your company) to come up with a plan for how to maintain operations if your primary location is compromised. Help them understand the IT requirements of any backup location.

Few small to medium-sized businesses have the resources to set up an entire secondary site that's ready to takeover in an emergency, and few are willing to spend the extra money for space that's empty most of the time. It's more likely that you'll pick someplace you already own or someplace with power and Internet access that you can use temporarily—usually a hotel, living room, basement, business partner's home or office, whatever works.

Of course, the size of your business is a major issue here. The suggestions above may be used in an emergency for smaller companies, but they may not be feasible for a larger one. Larger companies may need to invest in secondary space to use in an emergency, depending on their tolerance to downtime.

Power

Power goes out for many different reasons—not just because of natural disasters. But whatever happens, you absolutely need it to work. Power can go out during lightning, snow, and wind storms, and even if the overall power demand in your area is too high. Since no one can work for long without power, you may consider buying a backup generator, especially if you're in an area that's at high-risk for disasters.

Public Utilities

It's easy to think about the IT side of dependency because it's right there in front of you. The things that are easiest to overlook are public services, Internet providers, domain providers, and so on. You've already documented all of these, but what can you do to create redundancies that will eliminate these dependencies?

With regard to phone lines, consider planning ahead by having a voice over IP line that handles phone calls when the regular phone line is down.

It's great to have a secondary option out of state. As long as you have Internet access, you'll get calls (we'll get to Internet service in a bit). Any company in the state is going to be affected by what's going on, but those out of state probably won't. Having at least two options for each service is important if you hope to create maximum uptime.

Internet Access

Having voice over IP is great but it creates another question. What if your Internet provider is down?

Similarly, you can save some money by moving certain things into the cloud, but as you do so, you increase your dependence on the Internet. One solution is to have a secondary Internet provider.

If you do rely on the cloud, be sure to keep in mind that the Internet is now critical and that the business probably needs another line. It's another fee to think about, but now you've got a backup. Don't rely on a single company, use two and use totally different networks to remove or greatly reduce the risk of not having access.

Most firewalls can be configured to automatically failover to the secondary Internet source if the first one disappears, so the interruption in service is usually minimal.

People

Making sure multiple people can perform the same essential tasks is another form of redundancy you should think about. In the beginning, we encouraged you to gather a list of all the people who might be involved if a disaster occurred. Now is when that information will really pay off.

Just as with systems, services, and equipment, you simply can't rely on any one person in a disaster.

Assuming you've carefully followed the documentation steps above, you *should* have the essential contact info for everyone you might need, but now is the time to make sure, not during a disaster. Can you contact everybody you need to?

Of course, there are plenty of reasons why an employee may not be available when a disaster strikes. With that in mind, consider training backup employees for critical tasks. If those tasks involve gaining access of some kind (signing into services, opening a safety deposit box, etc.), make sure the backup employee has the necessary credentials or hardware to be successful.

Education is crucial. If one of your technicians is sick when there's a disaster, can another technician easily step in? Again, your documentation is key here. Consider dedicating one person on your staff to taking care of updating backup and disaster recovery plans and making sure everyone in the company who needs to access it can.

Having at least one person in charge of backup and disaster recovery plans will ensure that the plan is up to date most of the time, but having two keeps you covered even better. So if you can, decide on a couple of people that can handle backup and disaster recovery revisions and updates so that everything's ready to go all the time.

Testing can be a massive pain—who has time for that?

Before we discuss testing, make sure the documentation you prepared at the beginning is updated to reflect changes and additions you made going along. Once again, keep everything current and assign the task of keeping things current to a few different employees, if possible.

Testing can be inconvenient, so it's important for relevant members of your company to understand what you're planning. In some cases, you may even need buy-off, so take your fresh, up-to-date documentation—which now features backup and recovery procedures—to the same group you've been working with through the process and explain when and how frequently you'd like to test, along with everything the tests will entail.

It's possible an executive won't want to test. Many business owners just want to trust that what you're doing will work. It's a nice thought, but you should insist that you can't do your job without testing. Schedule a time on the weekend or after hours and get it done. You don't know what you're missing until you do.

Once you finally get the time to test things out, you've got to write down what went wrong, what went right, and what could be improved. After that, you've got to update your current documentation with the changes you've made so that everything is once again completely up to date.

Bear in mind that you will make a lot of changes to you IT environment as you move forward.

Any changes made in your documentation should also be noted in your backup and disaster recovery plan. Anything you leave out might cause you problems in the future, so up-to-date documentation is paramount.

All this documentation seems like a lot of work, but remember, if you do a little extra work at the beginning, you'll save a ton of work (and money, and your company's butt) in the end. It's the only way to identify what you have and what you need.

Ultimately, you can't do anything without it. You are solely dependent on your ability to write down every single thing you might possibly need, and your ability to keep this critical information safe, accessible, and up to date.

Once you've written down everything you can find, and you have backups and failover options in place, you should have no trouble at all handling any type of failure with efficiency and ease.

And that's just good for business.

Authors

Guy Baroan is the founder and president of Baroan Technologies. Guy uses a combination of over twenty years of IT and business experience in his role as the senior solutions engineer at Baroan Technologies. He also keeps his business on the cutting-edge of technology by taking part in industry leader forums and advisory boards.

Casey Morgan is the marketing content specialist at StorageCraft. A University of Utah graduate and lover of words, his experience lies in construction and writing, but his approach to both is the same: start with a firm foundation, build a quality structure, and then throw in some style. If he's not arguing about comma usage or reading, you'll likely find him and his Labrador hiking, biking, or playing outdoors—he's even known to strum a few chords by the campfire.

StorageCraft Technology Corporation
11850 S. Election Road, Suite 100
Draper, UT 84020

www.StorageCraft.com
1.801.545.4700
contactus@storagecraft.com