

12 THINGS YOU CAN DO TO STRENGTHEN YOUR COMPANY'S BUSINESS CONTINUITY PLAN.

WHAT IS A BUSINESS CONTINUITY PLAN?

In a profession where anything can happen, it's not a matter of if a disaster will strike, it's when. That's why a business continuity (BC) plan is so important. A BC plan lists the procedures a company follows to get back on its feet after the worst happens, covering processes, assets, human resources, business partners and more.

HOW IT PROS IMPACT THE BC PLAN.

A BC plan is quite involved and features input from every department in the organization. While IT teams should know the overall BC plan, their main obsession is always a disaster recovery (DR). A DR plan is specific to all matters IT and part of a company's overall BC plan. As you'll see, these plans require lots of thought, study and practice, so that when the time comes teams can efficiently rebuild and/or restore an IT infrastructure after a catastrophe.

See the DR steps you can take to influence your organization's BC plan.



STEP 1

START TALKING.

Have a chat with the people who depend on you to keep the network running. Start by asking questions at every level of the company to find out what systems are most important to maintain during any type of outage. Ask, "What systems can you absolutely not go without?", "What are your business function priorities?", and "What is the maximum downtime your department can live with before it starts hurting the business?" Answers to such questions will help you create the processes needed to recover critical pieces of your infrastructure.



STEP 2

PERFORM A HARDWARE RISK ANALYSIS.

Know exactly what you need to protect and replace. Create a detailed list of hardware, the original cost and today's cost to replace it (including outside vendor delivery and labor, if applicable). Next rank how critical every piece of equipment would be if it were to go down by assigning values to each item. The number of values assigned can depend on infrastructure complexity. Some IT managers use a simple "1, 2, 3 approach" whereby 1 is most critical and 3 is least important. Others rank from 1 to 10 or use a color-coding scheme. Pick one that works best for your team and network.



STEP 3

DIAGRAM YOUR ENTIRE STRUCTURE.

Document how the network is configured so that it can be replicated. Identify network switches, cables, PBXs, PDUs and routers and have backups. Keep resilient components on hand (and if possible at additional offsite locations) for what matters most, such as server rooms, core networking and large offices, so critical infrastructures aren't impacted during a crisis. It's vital to have **redundant power** at the ready, as networks that employ redundant UPS backups are more likely to avoid downtime.



STEP 4

SEPARATE INFO INTO TWO PERFORMANCE CATEGORIES.

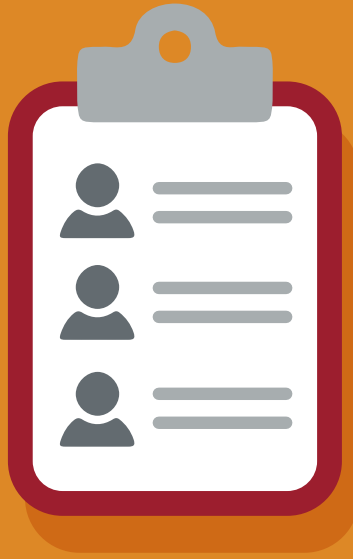
As an extension of the Hardware Risk Analysis, further divide your assets into “Must Have/Business Critical” and “Temporary Downtime” buckets. You can’t fix everything at once, and this process helps keep procedures organized and aids in determining recovery timelines. Implement either high-availability HA or quick-recovery technologies (such as replication or clustering) for critical apps (either between multiple office locations or to an offsite provider).



STEP 5

AGREE ON DISASTER RECOVERY TIME PARAMETERS.

Every disaster is different. Identify disaster types and assign rough response times for each step of the recovery. As a point of comparison, an unplanned power outage might require an hour's time to notify staff and properly shut down systems. But physical damage to a network due to hurricane flood waters could take days or longer to address. While there's no precise way to judge how long it will take to get systems back online, creating a general range helps improve resource and time efficiency.



STEP 6

KNOW YOUR CONTACTS.

There's no time during an emergency to hunt down contacts. Names, landline and cell phone numbers, email addresses... anything that you'll need to refer to at a moment's notice should be on a list. Record every vendor you work with currently as well as the customer service information for your network hardware. (Some IT managers cross-reference this list with the inventory from the Hardware Risk Analysis.) Make sure the list is easily accessible during an emergency. Everyone on the IT and HR teams should have a copy. Keep an additional copy offsite as well.



STEP 7

BACKUP DATA.

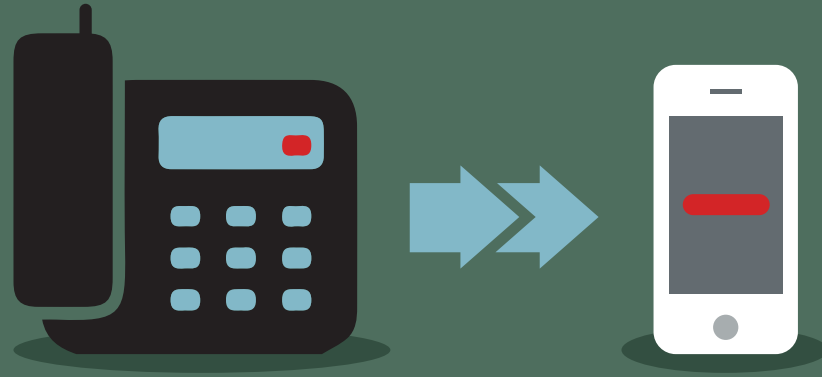
Rule of thumb: back up everything. Back up both the server itself and, ideally, specialist applications (such as Exchange) separately. Refrain from tape backups; power management software allows for graceful shutdown to local disk-based storage and has tools to migrate live workloads into cloud-hosted backup environments. The key is to assure that stored data is not associated with your physical places of work because you may need that data to create temporary IT networks.



STEP 8

PLAN TO CREATE TEMPORARY OFFSITE NETWORKS.

Prepare to work out of temporary structures should main places of business require restoration. Explore as many off-site options as possible and have hardware at the ready, even if from third-party providers. Critical to the plan is the transportation of hardware and personnel to temporary networks. Work with transportation vendors locally and out-of-state; this is important because a major weather event can take out the transportation businesses close to you as well. Consult with HR to make sure mission-critical staff will be made available.



STEP 9

REDIRECT VOICE.

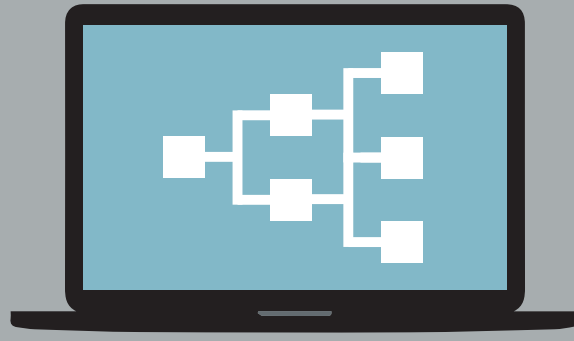
Telecommunication is perhaps most essential during the first hours of a disaster. It may take hours or even days to set up temporary places of work after a serious event, so it's a good idea to have a system in place that diverts calls to a different location with minimal notice. Consider diverting incoming calls to a third-party provider who can help explain the situation and provide information as to when regular communications will be restored.



STEP 10

VIRTUALIZE YOUR OPERATING SYSTEM

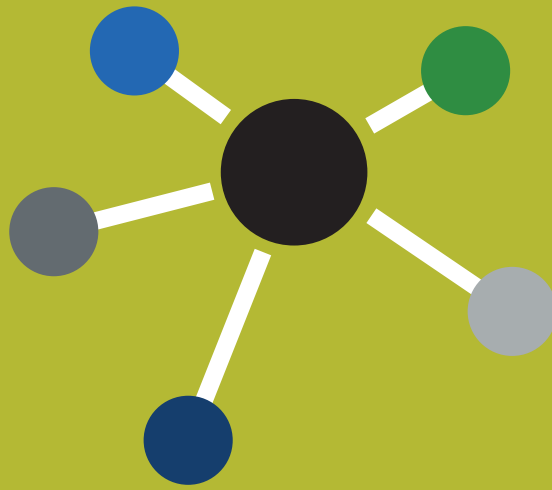
Virtualization adds a layer of agility and resiliency to your IT environment as it abstracts computing loads from resources to “unstick” the IT environment in space. In this way, “whitespace” is wherever the load runs at the time, making DR easier to implement, cheaper to run and more reliable when the time comes. Consider **integrated power management software** to connect agentless systems to **virtualization management platforms**. This allows complete automated control at the virtual machine level.



STEP 11

ADD POWER MANAGEMENT SOFTWARE.

Combining virtualization technologies with power management software (PMS) can help reduce the damages associated with downtime and may even eliminate disaster from happening in the first place. Event-based PMS software orchestrates the move of live workloads to safer locations without interruption to users — be it another rack, room, or facility. A dependable PMS package can trigger a recovery platform, such as **VMware's Site Recovery Manager**, to initiate a fully automated relocation of a primary data center to the backup site without the need for user involvement.



STEP 12

USE A NETWORK MONITORING TOOL.

Mitigate threats before they become full-blown disasters. Because problems can happen any time of day, it's important to install **network interface cards** that allow for direct connectivity to the network in real time. These systems allow for UPS control across the network via a standard web browser, SNMP-compliant network management system or power management software.

GET STARTED.

The rule of thumb: A good DR plan isn't about getting everything up and running immediately. Instead it allows your business to do enough to function and serve customers without letting on that normal systems are down for the count.

Want to set up your own DR plan? Start with our **Disaster Recovery Checklist**.