CONTENT PROVIDED BY

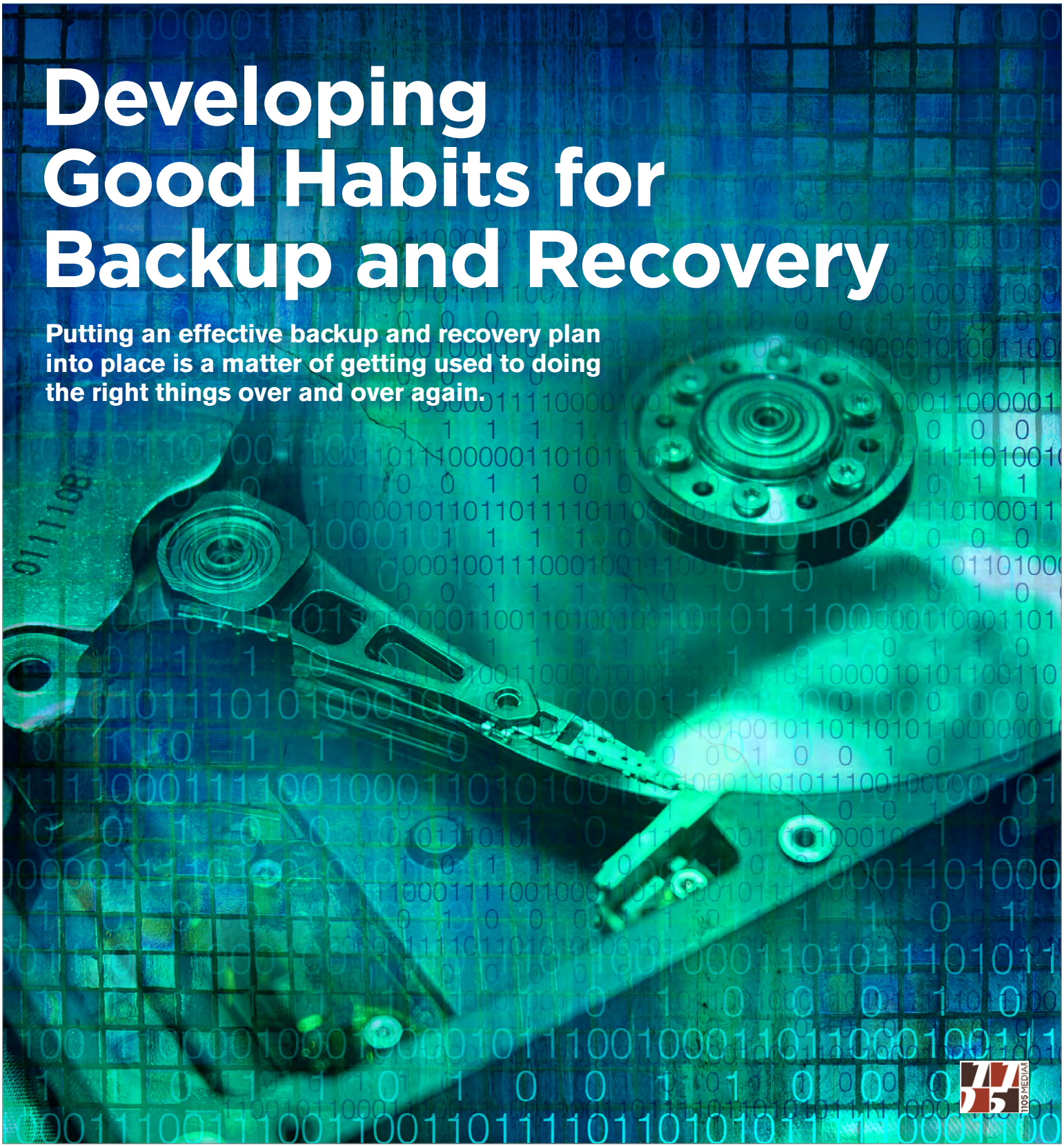
Redmond
THE INDEPENDENT VOICE OF THE MICROSOFT IT COMMUNITY

SPONSORED BY

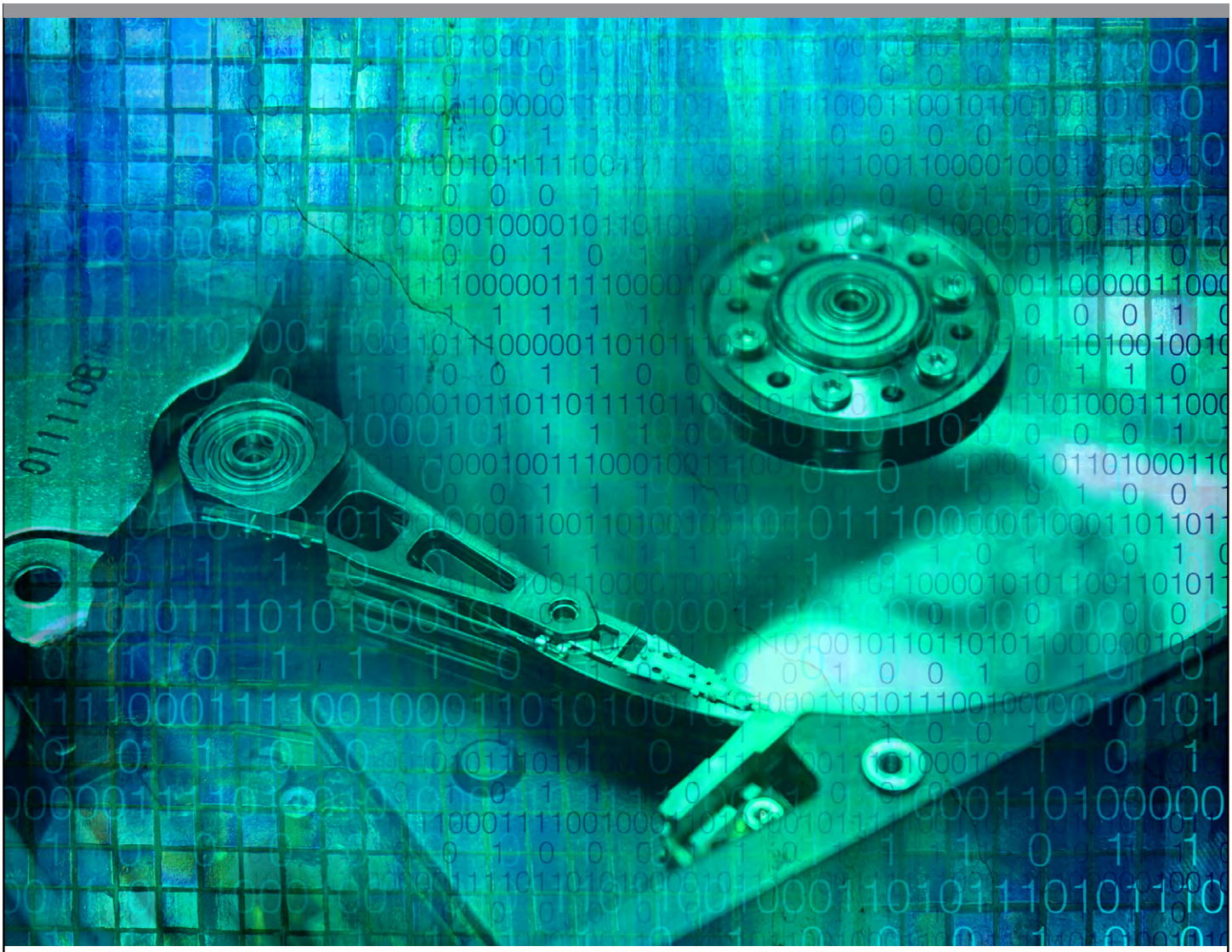
DELL

Developing Good Habits for Backup and Recovery

Putting an effective backup and recovery plan into place is a matter of getting used to doing the right things over and over again.



1105 MEDIA



Developing Good Habits for Backup and Recovery

BY DEREK SCHAULAND

Information is an organization's second-most valuable asset, next to its people. It's a bit surprising how many companies still struggle with backup and related activities. Whether the issue is the backup process, the recovery process, or trying to find the best and easiest solution to help improve the backup and recovery experience, it is something that causes a fair amount of heartburn. In this paper, we will look at some of the types of backup available as well as outline the importance of testing backups regularly to ensure they work when needed. After all, backups are only as good as their recoverability; if you back up everything every day but cannot recover when needed ... the backups are not doing any good.

In this paper, I will be digging into backup and recovery from a high level with a goal of determining the good and the bad, hopefully to help build better habits around backup and recovery with the business in mind.

Continuity and More Continuity

I work in an organization that has a lot of information and data. All of the data is backed up, and recovery happens once in a while (admittedly not as often as I would like). Paper is also a big part of our data story, and even though bringing the "paperless" concept to business would be the coolest thing ever (aside from faster Internet), it is something that may well not come around. I am sure this is no different than most organizations; in fact, because it is so common, it makes a good case. The goal of IT is (or should be) to help the business move forward with whatever it is that the organization does, crank more widgets, build better software, publish more interesting content … Anything that is important to the business is IT's mission.

Disaster recovery helps to enable business continuity by allowing a failover to occur to another location so work can continue.

What about keeping things moving all the time? Sure, there are backups, and we have those to chase down data when files go missing or become corrupt, don't we? If there is some kind of disaster, natural or other, there must be backups in a useable location to help get things moving again. In addition to keeping the business moving and functional, think about all of the idle time that will manifest itself during any kind of downtime. Sure, if the Internet is down for five minutes, it is likely that people will see it and wonder, but they can probably continue working. When you need to recover information that is missing to ensure that orders can process or items are visible, people will need to wait a good amount of time for that to complete. In this case, they will have idle time while waiting, which costs the organization money on top of the processing or business that cannot complete.

Disaster recovery helps to enable business continuity by allowing a failover to occur to another location so work can continue. This may not solve all of the issues caused by a disaster, depending on the nature of the organization, but it will help get things moving again quickly or keep them moving so that there is minimal disruption.

Testing All the Things

So, now we have considered how important it is to make an effort to have data moved offsite for continuity's sake, and the data is landing

over at the DR site as often as needed. Everything is perfect, right? We can get the things we need when we need them, and there is no need to look at this any further? This may indeed be the case, but there still needs to be testing to ensure that your offsite replications are working. Remember, if a backup or replicated backup cannot be recovered when it is needed, it doesn't serve the ultimate goal of being useful to the business.

Making sure that things are backed up for immediate file recovery and that back up offsite for disaster recovery happens regularly, as should the testing of these solutions. Keeping a regular and published schedule of testing for backups and DR will certainly help with this. If your co-workers and business management team are aware of what you are up to and this is known well in advance, there will be less interference with the process and fewer surprises to the IT team when the time comes to complete the testing.

If a backup or replicated backup cannot be recovered when it is needed, it doesn't serve the ultimate goal of being useful to the business.

An example testing schedule might be once per quarter on the third Saturday of the month from 5:00am-9:00am, or an appropriate amount of time for your process. Scheduling these and posting the information will help keep questions at bay about when people can get back to work or continue what they are used to doing. Maybe the cutover lasts a few days and the company works from the cutover site for a while, and the initial interruption is over in a couple of hours, then things resume. In either case, the more people know about what is going on (such as in the case of a disaster recovery test), the more OK with it they are likely to be.

Organizational Buy-In Isn't Always Easy

All of the discussions about backup, restore, and disaster recovery are great as a concept because they allow the IT organization to consider what might befall it in the event of a disaster. Once a few situations are fleshed out, the IT leaders can begin the task of selling this project (or projects) to management. Selling backup and restoration of day-to-day files will be pretty easy. Remember, everyone who has used a computer has lost a file or needed to recover from an accidental deletion. Users will call the help desk to do so, and if it is impossible to recover due to the simple fact that no backups are being done, red flags will go up all over the company. If the person calling is the CEO and you cannot recover her files for

these reasons, there might be trouble. The only good news there is that it likely won't take long to get moving on a backup solution to solve the problem in the future.

Disaster recovery, on the other hand, might take more convincing. It shouldn't be a hard sell because you are planning to keep your data safe from things beyond your control. If a tornado takes out your datacenter, there has to be offsite storage of data somewhere else to allow business to get back up and running with minimal interruption. If there is no offsite copy available, someone will have to explain to the business owners and project teams why they cannot just continue working from another location, and it will likely fall to the IT group to pass this news along.

If a tornado takes out your datacenter, there has to be offsite storage of data somewhere else to allow business to get back up and running with minimal interruption.

There are all kinds of excuses for not worrying about anything offsite, ranging from, "We don't have that much data" to, "A disaster isn't going to affect us; the building is built to withstand that stuff." If the building is destroyed, it hasn't withstood much of anything, and it will be too late.

Disaster recovery is something I would consider expensive just looking at the cost of another data center and servers and the expense of IT. But keeping your data somewhere else in the event of a failure, even at inflated costs, is cheaper than losing your data. Without information about the products you make, there is no real ability to make products that will meet the needs of the market because you no longer know what the market needs. If your entire warehouse is destroyed, making some things to get the company started again is essential, but how will you start again with no plans or information?

Your organization has many important assets that help achieve its business needs and goals. The most important asset is the people who are employed there at every level, but the next is the data used to drive your business. Everything else is secondary and can more easily be recreated.

Building Trust and Getting Buy-In

We have talked about a number of reasons why backup and disaster recovery are needed and what they can bring to an organization. All that is left is getting there … getting the buy in from management and

really helping them understand the reasons that backup and restore practices are necessary, and then helping them see how disaster recovery can really save the organization's bacon. It is certainly not unheard of to think about disaster recovery like insurance; it is a cost to carry, and you hope never to use it.

Lost or missing files that can be recovered from a snapshot or a local backup taken last night are easy to explain. In fact, you could put together a demo to show the recovery of files from local backup to help drive the point home. It is possible to do this with DR as well, but not nearly as quick to pull together. You might be able to use a bit of space at a cloud provider to create an offsite environment that can be used as an example to help explain disaster recovery. Using a small environment with decent replication from a local computer would allow for this, and then bringing it to fruition would simply be a matter of scale. Since cloud computing continually gets cheaper, this might be a great way to help your organization move into a working disaster recovery practice. Using the cloud provider's datacenter and resources is significantly cheaper than building your own data center in the middle of nowhere to ensure the security and availability of information. In addition, having a completely offsite recovery solution can allow connections from anywhere. This way, your workforce will be able to get back to their mostly normal routine while construction of the new corporate headquarters is just getting started.

It is certainly not unheard of to think about disaster recovery like insurance.

Recommendations

Here are some steps your IT department can take to find out more about the organization's disaster recovery and backup practices and what might be possible if there aren't any:

- Talk with IT and business management about what is in place currently.
- Talk with other members of your team about how backups are done.
- Test how backups work at planned intervals and small, medium, and large scale. Begin by recovering a couple files to another location, then a department's information, and finally a server's worth of information to see how the process works.
- Ask about offsite storage and disaster recovery.
- Review planning documents concerning disaster recovery and talk through them with both IT and Business leaders.

- If there is no current disaster recovery plan (where there isn't one at all or the existing one is completely out of date/testing), work with the organization to develop a plan of action and budget to follow through.
- Work through and document the final plan before any implementation to get everyone up to speed.
- Begin implementing the disaster solution and documenting the process to make note of difficulties.
- Once the recovery site is up and running, be sure to keep detailed schedules and plans for testing visible to everyone in the organization. They should know from day one that this solution will be tested and the schedule of the testing to avoid any surprises that might cause testing to be skipped.

Backup and disaster recovery do not have to be scary topics, but many times they are seen as just that.

Backup and disaster recovery do not have to be scary topics, but many times they are seen as just that because of the nature of the work involved and the possibility that something will be missed and those associated with the project will be blamed and maybe fired. Just remember that your coworkers will be very thankful for your ability to help them recover files or in the worst case and get back to work as soon as possible. An IT organization that takes the lead on these projects should be seen as one that cares about its business and is willing to take steps to ensure that it can continue operating in the event of a disaster. Any effort and planning put into disaster preparation will be worth its weight in gold if recovery is ever needed. R

Derek Schauland has worked in technology for 15 years in everything from a help desk role to Windows systems administration. He has also worked as a freelance writer for the past 10 years. He can be reached at derek@derekschauland.com.