Small Businesses and the Importance of a Backup Plan

Stephen Macpherson, Sales Director

It doesn't matter if you're a small one-man show, or a large multi-national: no doubt you will be heavily reliant on technology to support your operations. Your customers are very digitally aware and interact with you through common routes such as the internet, email or electronic ordering interfaces. Much like Macrium in a lot of ways! For a small business it is a lot of effort to establish and maintain the technology to support the systems needed for sales, marketing and support; that is often when the needs of data security, or a business disaster recovery (BDR) plan are overlooked.

There are a lot of surveys, vendor reports, expert recommendations and case studies that highlight the need for a BDR plan, yet many small businesses regard it as too difficult or even too expensive. This is despite the enormous monetary impact of downtime on a small business and how this is often fatal to the success of the business owner.

There are at least five good reasons for having a BDR plan:

1 Systems (hardware and software) fail - Still the most common cause of data loss

"Recently, both disks of a raid-1 set failed at the same time. Macrium was a lifesaver. We have completely restored the most recent image of the service and we used the more recent backup done the night before to restore all the data. Almost no data loss. Client was very grateful. This was a hardware test for the Macrium Server software and it passed in the best possible way!"

2 Lessens impacts of cyber-attacks – an area that is often in the press today

"I had a client that had been injected with the CryptoLocker malware and did not let anyone know until 4 days later. By that time most of our backups had been encrypted as well. Luckily we had one drive left that was untouched. We were able to restore from that and bring the office back online."

3 Keeps client data safe – loss of client data can be more than just embarrassing. It destroys business reputation and can cost vast sums to get that data back

"One customer had a $450m database of investors. The company who set up their backup did not check it and when the hard drive failed, there was no backup on the 3 different systems that were setup. I had to send the drive away to get the database off it."

4 Protects against effects of natural disasters – everything from lightning strikes to fires and floods. Acts of God can hit at any time!

"The client's building burnt down. He did not have off site backup, instead he relied on a local backup to an external hdd which was kept in a fireproof safe on premise every night. The safe unfortunately was not waterproof…! In putting out the fire, the fire department flooded the safe, damaging the external hdd. We had to send the drive out for professional data recovery, costing the client thousands of dollars in expenses, on top of lost productivity for the two weeks it took to recover the data."

5 People make mistakes – the second most common cause of data loss

"Photographer saving RAW images only to a 3 TB external drive. Drive got knocked off the PC it was sitting on while being accessed and damage to the heads resulted. $1300 recovery which could easily have been prevented with a larger internal drive and Macrium Reflect."

At Macrium our support and sales teams come across all kinds of horror stories on data loss and not surprisingly we strongly endorse the need for a robust BDR plan. Often we hear good news stories where a small business owner was able to recover quickly and effectively from a major data loss, underlining just as much the need for a plan. At Macrium we often use the "CIA" model to define data security in three areas; Confidentiality, Integrity and Availability. Backup can address all of these areas but is most directly applicable to ensuring data availability and integrity.

What makes a good backup solution and what should small businesses consider when selecting a solution? We recommend they look at the reputation of the vendor. Are they well thought of in the market place? How do business and home users rate them? Then also consider pricing scalability, compatibility, support and ease of implementation. However, we recommend that above all they need to select fast and reliable solutions. Our research and the feedback we get from IT professionals is consistent and clear. Speed and reliability are the two most important factors when considering backup technologies.

A BDR plan is more than just buying technology. It needs the culture of the business to understand and implement the "CIA" model and make sure they address data security in all three areas. The final message is, be prepared! The unrealistic optimism that it will never happen to you, or just leaving it for another day is dangerous. It is too late when disaster strikes because the cost and disruption of data recovery often leads to loss of reputation, customers and possible business failure.