

SMBs Continued Challenges with Business Continuity & Disaster Recovery

Speakers: Michele Ogle, Infrastructure Solutions, IBM
Jeffrey Hill, Aberdeen Research Analyst, IBM

Michele:

Hello this is Michele Ogle with IBM Infrastructure Solutions. And welcome to this segment of our podcast series for SMBs. This segment is focused on SMBs Continued Challenges with Business Continuity and Disaster Recovery.

In today's environment threats to a businesses operations range from blackouts, to hackers, to natural disasters, and size doesn't matter. Large, medium, or small companies must make the necessary investments to minimize damage and disruptions to ensure long term vitality, as compliance to changing industry and government regulations and the need for a coordinated approach becomes evident. Having a Business Continuity and Disaster Recovery plan or a BCDR plan, is the key to achieving that. But for SMBs who have limited budget and skilled resources, the lack of planning, and the risk associated with it is significant.

Joining us is Aberdeen Research Analyst, Jeffrey Hill. Jeffrey has looked at the Best Practices of companies around BCDR and how data management through virtualization, storage, backup, archiving, are keys to success.

Hi Jeff how are you, and thank you for joining us today.

Jeffrey:

Hello Michele, pleasure to be here.

Michele:

You know Aberdeen has done a lot of research in this area. And I know you've had a lot of experience as an analyst in this area as well. Would you share with us a little bit about your experience and Aberdeen's research approach?

Jeffrey:

Sure, actually the Aberdeen's methodology is based on the concept of surveying end users on a particular topic, in this case Business Continuity and Disaster Recovery. And we use something we call the PASE framework. And those letters just stand for the pressures and the strategic actions, the organizational capabilities, and the technology enablers that an organization would bring to bear on trying to solve a business problem. From that we drive something we call the Maturity Framework. And the Maturity Framework is simply a division of all the respondents into what we call the Best in Class, which is the top 20% of our performers. The 50% is our average class, and the 30% is the laggards.

If you go to slide 4 what you see is that we then compare the performance of the Best in Class to the other, to their peers, to the other classes, and we talk about how the average class and the

laggard class might achieve Best in Class status by using some of the processes and Best in Class practices that we talk about in our research.

Now to set the stage if we go to the 5th slide, these are the overall (inaudible) demographics. This is not specific to the SMB but to the overall participants in the survey. And what I want to direct your attention to first of all is the lower left corner, we had a very good (inaudible) participation from North America which is typical. We also had an excellent participation from Europe, the Middle East, and Africa, and a significant participation from Asia Pacific. And you'll note in the upper left corner we have good representation of both Senior Management and IT Staff, and IT Managers. So the people who answer the survey are the people who are either charged with implementing Disaster Recovery or setting the strategy for it.

And finally over in the right hand corner you'll see that we had a very good participation from what we define as the SMB, which are businesses under a billion dollars in revenue, which represent some 71% of our respondents.

Michele:

Jeff this seems very comprehensive. So there's no question that every things not making guess work out of this stuff; this is a serious process that you have here that covers just about every measure that we can. Let's talk a little bit about how this approach has been used in the area of BCDR and SMB.

Jeff:

One thing we need to talk about I think is how much participation or how many people in the SMB, how many companies in the SMB, have implemented what we would call a BCDR plan. And you'll note on the chart on slide 6 that in fact we have good participation. But at the same time 44% if you include people who have no plans to implement, or people who are planning to implement that 44% of our SMB respondents have not yet implemented any kind of Disaster Recovery plan. And that's a very significant number and certainly the topic of which we're focusing today.

Michele:

Yes I was going to pull that statistic out myself and kind of throw it out there at you because that seems like a really high number. You know 44% not having anything in place and 42% of those people still in the planning stage, meaning I'm going to get to it eventually. So what you know what's keeping them from getting to actually creating a plan? Why is that percentage so high?

Jeff:

Well if you go to slide number 7, these are the responses from the SMB respondents. They're asked to pick the top two challenges that they face. And by an overwhelming percentage understanding the scope and complexity of the BCDR plan or the system, was by overwhelming percentage the biggest barrier or the biggest challenge to adopting BCDR. And then followed very closely by anticipated costs and finally lack of internal expertise. I think these are very significant numbers because what they say is that either our SMB customers don't understand the depth and breath of the plan or the amount of planning that's required, or they are concerned about their own ability to implement such a plan.

Michele:

You know I think so. And when we look at the fact that understanding scope and complexity is such a high, so high on the list of the key challenges, it kind of makes you wonder if part of the issues that there isn't really a clear definition of what a real BCDR plan is out there. And maybe they're looking at it in pieces and parts. Based on your research and experience Jeff, how would you define a Business Continuity and Disaster Recovery plan?

Jeff:

Well the term Business Continuity and Disaster Recovery are really two parts, two elements of the plan. The first part Business Continuity refers to a formal plan that embraces all aspects of an organization and which talks about how to continue the business in the face of an interruption or some kind of event that would cause a problem.

The Disaster Recovery part of the BCDR plan is perhaps a lot easier to understand because it's focused on technology as opposed to planning. But the two functions together are really what defines a Business Continuity Strategy and a Business Continuity Recovery plan.

Michele:

And it sounds like you really shouldn't have one without the other. Right you know they're not mutually exclusive, they're meant to be together. You know now that we've got a definition and I'm thinking some folks may have needed that. I know it was helpful for me so thank you. But now that we have a definition I'd like to ask you to outline a few steps that our small and medium businesses would need to take into consideration in order to get started and get down the road of actually creating what we've defined as a BCDR plan.

Jeff:

Well if you move to slide number 8 what you see is some of the steps that people who have already implemented BCDR have taken in the SMB, and obviously the first focus 58% is on creating an infrastructure for Disaster Recovery. So focusing on the technology portion of the plan, but the very second and equally important item is establishing a formal plan. So with those two in mind that really is the basic two steps required. We'll talk a little bit about some of the other aspects of a plan as we proceed.

But you'll notice that the next two items from the SMB were updating or changing an existing plan or standardizing Disaster Recovery procedures throughout the organization. And I want to make a point here which we'll discuss again, that any Disaster Recovery and Business Continuity plan has to be one that is a living document; and needs to be modified as the business changes and to accommodate changing business conditions.

Michele:

Yes I think it's not a set it and forget it kind of thing right. You have to go back and tweak it and make sure that it's related to your existing circumstances and environment. Now for those SMBs that do have a plan, the guys who have taken the time to at least begin to get down the road, what are you finding are some of the key activities that make up that plan?

Jeff:

Okay if you'll go to the 9th slide, we asked SMB our respondents that question. And the most important activity was of course backing up physical data on servers. That's the key to recovery and rapid recovery.

Again if you move to the third item on the list, Off Site Storage, again a way of making sure that if your business is interrupted for any length of time, or if your primary business site is unavailable, that you have an offsite way to recover business data.

And I want to note that the last item, Regular Meetings of a Business Continuity Team, while it's the smallest in terms of percentage, again it's probably one of the most important. Because this gives us the notion that a regular meeting of the people who are responsible for making sure that the Business Continuity plan reflects the current state of the business and that Disaster Recovery Infrastructure works correctly, is critical in making a plan successful over the long run.

Michele:

Yes I would like for us to touch on that a little bit later because that sounds like the people side of this. You've got the technology side and the people side. Let's stay on the technology side for a minute. You know we see that backup when you (inaudible) those lists of activities, you know the majority of it is about backing it up and getting the information. Talk to us a little bit about the technologies that companies use, current technologies and even previous technologies are still being used. Especially around virtualization because I know that's one that I hear about all the time.

Jeff:

Sure well slide 10 shows us some of the technologies that are currently being used by the SMB to support their BCDR plans. And you'll see once again physical tape is the predominant way of backing up and restoring critical business data. That's very interesting because physical tape as a medium is a very old medium, and yet it is still astoundingly popular, not only with the SMB, but with businesses of any size, physical tape still is the predominant way that people think of preserving data. However physical tape does have some limitations in terms of rapid recovery of data. And so the second two technologies, disk to disk backup and disk mirroring, address the idea of applying technology for rapid recovery of critical applications, email servers, our customer service applications, and so on, need to be up as quickly as possible to make the business operational from a systems standpoint.

Notice at the bottom there are two, there's one new technology Virtual Tape Library which is in fact a growing substitute for physical tape although it has rather different qualities. And certainly the option of using an offsite or managed backup service maybe an option for some SMB customers, particularly ones that haven't necessarily built a physical infrastructure support BCDR at the present time.

Now on the next slide, slide 11, I'm talking a little about why virtualization is changing the landscape of BCDR, and it really does so in several different ways. It offers us new ways to capture the current state of a server by using something called snapshotting technologies or some times that's called continuous data protection. Multiple snapshots can be taken of a server over

time. And so it's possible for example to automatically backup something like your accounting data on a regular and formal basis, such that you can go back in time and retrieve an image of the data and the application. Also in that same vein the use of D duplication technology, which is literally taking data and removing the duplicates, is a way to remove redundant data from the backup and to make the backup smaller and thus easier to manage.

Virtualization allows fewer dedicated servers in support of Disaster Recovery. It makes management of the infrastructure somewhat similar. And it offers something called Bare Metal Recovery, which allows the server data and the image of the server to be restored to another server even if the server has no operating system or is not of the same type as the original server. So there's some flexibility that's been introduced by virtualization, which promises in the long run to lower the cost of building out a Disaster Recovery Infrastructure.

Michele:

Now Jeff I just want to stay on the virtualization topic for one more minute. How easy is this to do? I mean I'm assuming that many servers today include this technology. Is this something hard for SMBs to begin to adopt?

Jeff:

I think that, I think the answer to that is I don't want to over present the case for virtualization either. I think virtualization there are some vendors who are promoting the idea of sort of a virtual appliance, which would make it easier. Certainly this sort of one box solution is not, we haven't got that yet. But I guess my note would be if you're using virtual servers in your environment already, then it's relatively short leap of faith to use it for your Disaster Recovery Infrastructure. If you haven't started using virtualization in your business then that's going to require more expertise and at least for the moment that may or may not be a good decision for smaller companies.

Michele:

Well thank you so much for your insight on that. We always have to provide all of the aspects that are in front of us and choices. So thank you.

Jeff:

Absolutely.

Michele:

Moving a little bit past the technology to we've got the brand, we've got the technology, we've implemented it. It's not a set it and forget kind of thing; we've talked about that already. How important is maintaining the plan, testing the plan, and updating the plan?

Jeff:

In my view it's critical. If you move to the 12th slide what you see is that most of our SMB companies, 36% update their plan on an annual basis, some of them more frequently but certainly annual. What concerns me is the 28% that are not scheduling an update on a regular basis. And to use the words that you just used Michele, it sounds like they're setting it and forgetting it. Unfortunately and I can give you a very easy example, let's suppose that you add a

new branch office, or a new sales office in another city, if that office is not reflected in your BCDR plan, you stand at least the possibility of losing critical business data. So again not to reinforce this point too much but the formality and the regular review to update the plan so that it reflects the current state of the business, and maybe even the current economic state the business finds itself in, is a critical component of making a BCDR plan succeed.

Now that's only one part of the picture. If you move to the 13th slide, okay well we have a plan but are we in fact testing the plan? How do we know that it works? And again you'll see that the majority of the SMB customers test the plan yearly. But again this nagging 24% are not testing the plan on a regular basis. You might be surprised to find that the reason that most Disaster Recovery plans don't work is because the test to make sure that they work was never completed successfully. So a critical aspect, and this applies to an organization of any size, if you have the infrastructure and you have the mechanisms in place to perform Disaster Recovery, then you need to test it and make sure that it works. And I would say annually is probably not often enough. Especially if you live in an area where there might be power disruptions or weather related phenomena that might cause a significant business disruption, there you might be wanting to do it quarterly for example, or at least twice a year.

Michele:

Jeff would it be fair to say that every time you go through the process of assessing and updating your BCDR plan you should test it as well?

Jeff:

Absolutely, I think the two go hand in hand to make a successful infrastructure and appliance.

Michele:

One more point. You talked about the fact that they're not just testing it on a regular basis but they're not testing it through completion. Talk a little bit about that because they may be, are they going half way through their test and when they hit a speed bump they stop and they never continue to figure out you know once they fix that speed bump whether it works all the way through?

Jeff:

Well I've heard end users say that the testing process can be very, very difficult, and is often perceived as being, we know the data's backed up so what's the point of trying to prove that we can get it back when we know we can verify by looking at the tape or the media that we've done our backup on. We know that we can get, if we can get around the tape and we confirm it's there then it must be useable. Well I would be, I would suggest that the rest of the test is just as important as the first part; and particularly because Disaster Recovery generally is done in response to some kind of an event. The power goes out, a hurricane strikes, or a very simple example, last year in Boston someone was digging and struck a power line and there were businesses on a four or five block area that were put out of business for three or four weeks because they didn't have electricity. Now the time to test you infrastructure and find out that it doesn't work is not after the event.

Michele:

Not after you've gone down do you figure out whether or not it's actually viable to get back up.

Jeff:

Right, I think although it may be very difficult to test it thoroughly, I think it needs to be done. That's as critical as doing the backup in the first place.

Michele:

So looking at that, any more statistics that you wanted to share with us to help us keep some things in mind. I know that when we talk about backup you know recovery time of death is, are some key points around that. Anything that you've seen in your research that is notable?

Jeff:

Well here's a couple of interesting statistics on slide 14. These are talking about the average time it took for SMBs historically to recover their business to 90% functionality. And that average was 3.92 hours. Now to give you a frame of reference for that, the very Best in Class companies, and that would be irrespective of whether they were in the SMB or if they were in enterprise companies, was about three quarters of an hour. So four hours is not too bad. On the other hand if you're a business that runs close to your operational and you're worried about today's receipts, and logging business and placing orders, four hours is half a business day. And so you need to ask yourself, can I stand a four hour interruption.

Now another question we asked, well what would be your expectation for the amount of time it would take to recover to 90% operational functionality? And the answer was 9.7 hours. Now that's an expectation but clearly it's based on the previous statistic and their experience. So now we're talking more than a business day, more than an 8 hour business day, to get the business to 90% operational.

Michele:

That's a big difference.

Jeff:

Yes it's a big number and I would submit that there are many companies irrespective of whether they're in the SMB or not, that could not really afford to be down for a business day. That's a long time.

One other interesting number is the average amount of increase in SMB IT budgets for Disaster Recovery, which is only 3.2%. So clearly people are not, they're spending the money in other places, where they're not spending it as much as they might be to make sure that their DR Infrastructure and their BCDR plans will work correctly. So unfortunate statistics but that's what we're here to learn from.

Michele:

So take away from this, more budgets for BCDR plans and try to get your recovery point and recovery time objectives a little closer to Best in Class and not the average.

Jeff:

Sure I would agree.

Michele:

Great stuff. Now in the beginning we touched on the fact that the DR side of BCDR touches on technology, and then the BC side of it talks about process and people. So let's focus a little bit about the people side of things. We've got the technology stuff covered, but when IBM talks about BCDR planning and we talk about our approach, we incorporate the importance of people because they are the ones that are actually going to execute the BCDR plans. Someone has to flip the switch to get the backup done and get the restoration process going. So what guidance do you have here? Because I think that this is an area here that people forget.

Jeff:

Yes indeed they do. And if you go to slide 15, here are some of the Best Practices if you will that we get from our Best in Class. Clearly we've already established the point that Business Continuity requires more than just having a DR Infrastructure that performs. When we're talking about planning we need commitment and we need buy in from all levels of the organization. The time for the CIO to talk about the system, the infrastructure being in place and tested and working perfectly, but the employees, or staff, play a part in making sure that that plan actually gets executed. So a really good disaster plan would include not just recovery of data, but recovery of individuals, keeping employees informed. Notifying them of events that are occurring, people do much better when they have information than when they don't. And certainly it would be nice to empower people who are charged with making the business operate, empowering them to help in the recovery process.

And then I mentioned this before, updating the plan to reflect the current business conditions and realities. And you know we can't stress this enough, frequent and thorough testing; so all those elements really represent the idea that a successful Best Practice around BCDR involves both technology and people.

Michele:

And I would think Jeff that the people side of this becomes so much more important especially if you're a company that has remote workers and things of that nature. You have to take in to account those people where it may be difficult to communicate with them.

Jeff:

Sure absolutely. You bring up a very simple example. Many employees now would be able to work from home. So if the Disaster Recovery plan was so structured it would be very easy to switch to a remote site to support the operations of the company and allow employees to log in from home and continue to work and support the operation of the business.

Michele:

And that's where the Business Continuity part of the BCDR plan comes in right, keeping the wheels moving.

Jeff:

Yes absolutely.

Michele:

Well you know Jeff you have provided a lot of information, a lot of great information for us. This has been extremely informative for me and I believe for our small and medium businesses that are listening. Any last bits of information or food for thought that you'd like to leave behind?

Jeff:

Sure I've listed a couple of things on the 16th slide. Well first of all I think if you've been listening to this presentation you recognize that backing up alone does not constitute Disaster Recovery. That putting the tapes in the back of the car and driving them home, while it's a solution for smaller businesses perhaps, the point is that you need to have a purposeful infrastructure built around the idea of making sure that when something happens you're able to recover it in a reasonable amount of time.

I also think that it's important to understand that the effect of a disaster on SMB has in my mind a far greater impact. Because most SMBs don't have the resources to apply or perhaps even the special or focused team that who's only job is to make sure that disaster recovery is there. So from a technology standpoint I think the effect is harder on SMB than it might be on a large enterprise.

And then secondly the financial impact is much greater. Businesses of a certain size, larger enterprises, have multiple offices, they have great financial resources, they may have replicated datacenters; so in some ways even if they're not terribly well prepared in a Business Continuity sense, or a disaster planning sense, they still have resources to apply that a small business might not. And frankly they could absorb a larger shock than a small business. Again my example of the companies in downtown Boston, who and most of these are very small businesses, who really for a period for two or three weeks had no way to run their businesses. That's a devastating event for an SMB customer.

I think we talked a little about virtualization, so newer technologies are always impacting how we do business. And in the case of BCDR they are making BCDR more practical and more affordable. I think it's worth looking at some of the solutions that are available, again with the advisory that virtualization and similar type technologies may not be appropriate for every business. And sometimes the infrastructure that you have now if it's working properly, sometimes it's better not to look under the hood under you absolutely have to.

And finally I just put a quote here, I've heard this many times, I don't need to worry about Disaster Recovery because I don't live, we don't have a problem with hurricanes, or floods, or tornadoes, or power outages. Well I would suggest that you don't know what the next business interruption could be. Those are the obvious ones, and they seem to occur in certain parts of the country, but believe me no business is immune from interruptions. And with you not planning for disaster in some way, maybe disaster seems like a harsh word, but if you're not planning for

business interruption, and a significant one, then you're simply taking a chance and betting your business.

So on that note I will thank you so much Michele for inviting me to speak today.

Michele:

Thank you so much. I really do appreciate it. Thanks for sharing the Aberdeen Research which is great to see and see what is actually the state of the SMB marketplace when it comes down to BCDR, and your insights in this area.

And thank you for joining those of you who are listening to this segment of our IBM Infrastructure Solutions Podcast Series for SMB. For more information about Business Continuity and Disaster Recovery and IBM Solutions to help you plan, implement, and maintain your BCDR plan, go to www.ibm.com/expressadvantage/businesscontinuity. Thank you and have a wonderful day.