

Disaster Recovery & Business Continuity Planning

© emedikon 2009

Peter J Polack: Welcome to Medical Practice Trends' Expert Teleseminar Series. This is Peter J. Polack, M.D. In this issue we speak with Frank Polack, managing partner of Eviton LLC. Frank Polack has over 20 years in IT and project management implementation, consulting and training. His experience includes positions as Information Technology (IT) Director, computer aided design (CAD) Manager for the 1996 Atlanta Olympic Games and President of the Atlanta Chapter of the PMI (Project Management Institute). He currently directs the Project Management Office for a division of the Royal Bank of Scotland RBS World Pay.

Hello Frank.

Frank: Hi, how are you doing?

Peter: Good, so our topic today is going to be on disaster recovery and this is probably a topic that many medical practices are not familiar with, but in your line of work I'm sure you come across this a lot, particularly with the types of companies that you work with. So, can you explain to us exactly what is meant by disaster recovery and business continuity?

Frank: Sure, disaster recovery is something that's well known in the technology industry. Basically looking at how do you get your systems back online after some sort of disaster. There's all different levels: a disaster could be just one computer going down, its hard drive or power supply going bad. Could be a natural disaster, tornado or hurricane, flooding. So you have to look at the different types of disasters you might encounter and then set up plans that are appropriate for the amount of risk that you might face.

Peter: Now I read somewhere where 70% of disasters are actually caused by people.

Frank: Yep, usually, somebody knocking something over or erasing something or somebody outside that cuts the fiber coming to your building and your internet connection goes down. There's all sorts of things like that that are really more careless accidents that happen than the types of things like a tornado or flooding. So those are things that you have to look at.

I know that we had one client that was all set to move into a new building and the day before they were moving, their computer room sprinklers sprung a leak and luckily there were no machines in the room otherwise they would have had a really bad disaster. But that's one of the things that a lot of planning had gone into everything but that was one thing that nobody would have expected, because by that time they had received the certificate of occupancy and the sprinklers supposedly had been tested and they're not sure why one of them sprung a leak.

So disaster recovery is one side of it and the other side, the business continuity is, once a disaster happens, what do you do to get yourself back online? How you continue your business, either temporarily until you can get something running or just putting back the pieces in the same place.

Peter: So business continuity, there's actually insurance for that, is there not?

Frank: Yes, there's different types of insurance like that but basically insurance that would cover relocating to another building, any of the costs involved in getting you up and running. I mean you'd have to probably set up phones, set up computers. Again a lot depends on the level of interruption you've received. So let's take for example, you might be in a building where there's a small fire and part of the building got destroyed, so can you continue in that building? Can you continue your business there or do you actually have to relocate and see patients somewhere else, for example, if you're a medical practice? Part of your planning should probably be, where else could we go? Maybe striking up an arrangement with another practice that may allow you to see patients on a limited basis at their location until you get yours up and running.

Peter: There actually was a couple weeks ago here, there was a pediatric group, three doctors, and their office actually burned down and they had no sort of disaster recovery plan, so fortunately the medical society contacted a lot of physicians in the area and they helped out. Gave them a place to practice but it was nevertheless pretty devastating.

Frank: I can imagine. Especially when you start trying to find records and especially now going forward with all the HIPAA requirements and everything else, you kind of really have to be careful what happens with that data so you may even have lost data. I'm not sure how

that would happen legally but imagine a patient that has complications and you don't have any information on what happened.

So talking about plans, yeah, you have to look at the different types of disasters as I said earlier and the different levels and do a risk analysis. And that usually sounds like a pretty big task but risk analysis is relatively easy. You start sitting down and looking at the different parts of your business and just ask, "what if". So obviously the most obvious ones are what if our computers go down, what if we lose power to the building, those kinds of things. But there could be others. You could say, what if something happened down the street that would keep people from coming to my office? What happened in New York a few weeks ago, where a crane fell onto an apartment building. I'm sure those streets were closed for a least a week or more, so what do you do? Do you close down or do you go to plan b and go to another place.

Part of that is also the logistics. So how do you tell your patients to go somewhere else? How do you notify, where do you keep that information? You go home Friday and find out over the weekend that you can't get to your office. So how do you know who to call who might try and show up for an appointment?

Peter: And not just have this on a computer somewhere but also a hard copy, maybe a laminated sheet that's kept in each location in case there is a total power failure or a flood or something. A plan that's kept on a computer would probably be useless.

Frank: Yeah, unless you plan for that and have an offsite computer or some way to restore the data that you take home on a regular basis. At the minimal level you come up with a backup. This is really where you start out saying, okay, what happens if something fails in one of my computers, I lose a hard drive, for example, or I get hit by a virus? So, you have to have a way to backup your data and then come up with a plan on how often it gets backed up and what do you do with the backups. So, for example, you might do a backup every night where you swap out a tape every night and then on Friday you take whatever tape, that is, you take that home, offsite. And you just continue that every week and then once a month you take a tape and you put it offsite at a bank vault of something.

There's all different types of plans like that but you have to think of how much business would I lose if I come in the next morning and the computer's gone or broken.

Peter: That's actually the system that we have. We actually back up the data from both the practice and the surgery center, and the tapes are taken offsite by a courier who's an employee of the practice. That's also another issue that you need to look at is who has control of the tapes.

Frank: Exactly. I mean, again, what kind of liability would you have or who's holding it or what kind of information is on there, especially if it's got patient records? You hear all the time about somebody from the government who lost a laptop that had a bunch of information on it. Typically those are encrypted to where nobody can really get into the data that's there, but there's been cases where they've lost bags of backup tapes. So someone who could figure out how to read the tapes on a certain machine probably could look at the information.

So if you're backing up patient records with social security numbers and other health information, you have to make sure that either you have a reputable company that's keeping those for you or find a way to encrypt the data. You just have to make sure you have a plan and possibly even check with your lawyer to make sure you're covered from a liability perspective.

Peter: Yeah, our information technology guy also reminded us that it's important to test the backup system. There was a case of a practice that was using an automated tape backup system and when they had a server crash they actually found out that for the last couple of weeks the tapes actually had gibberish on them.

Frank: That's a very important part of having a backup system is actually doing test runs on a very frequent basis because you never know, just like anything else on a computer, a tape drive can go bad. And many companies actually have two or three tape drives and maybe alternate the backups; there's a lot of different ways to cover that. But again that's all risk analysis to say what if, what if the tape doesn't record one night? You know, something that happens a lot is at some point, the tape can't hold everything on a server and so you then have to put a second tape. Well how do you know that? And so there's cases where people have backed up and yeah, the first tape backed up with no problem but it didn't finish because it needed a second tape.

So those are things that have to be looked at on a very frequent basis to make sure that it's working and part of your business continuity plan should be to take those tapes and take them to another machine somewhere else and see if you can actually restore it because that's the other part of it. If your building catches fire and the machines are destroyed by water or whatever else, okay, you got a tape, now what? So you have to make sure you have an identical machine - at least the same kind of tape drive, the same kind of operating system that can read that tape and see if it actually does restore it to where you can actually run transactions on it.

Peter: That's a good point. Actually what we do is we take the backup tapes and they're used the following day on another machine that's used for training staff on the office practice management system. So that way they know if there's a problem with the data, that's the backup from the previous day.

Frank: Exactly, that's a great idea. I'm sure a lot of practices don't have that capability of having a training room or something on those lines but it is important that at least, at least once a month if not more frequently, they take a tape and make sure they actually can restore it. That's just part of your plan and again, when you start looking at large public companies that have all the problems with Sarbanes-Oxley [Act of 2002] and all that, that's part of the written plan that they have to show: here's how we're protecting that data and how we're making sure that we continue the business.

So for small practices it's definitely a good idea to do that and if they have an IT resource, they might just ask them to, here, we'll buy another tape drive, keep it at your office and just test these for us.

Peter: There's actually a nice book on this [topic] by Donna Childs that's called "Prepare for the Worst, Plan for the Best – Disaster Preparedness and Recovery for the Small Business". And the point that she makes there is that there's three key reasons why you should do this [have a disaster recovery plan].

The first is that having a disastrous recovery plan actually can reduce your insurance premiums. The second is that it forces you to look at the – well, for most companies it would be the supply chain, but in a medical practice it would sort of do an analysis of your cash flow, give you essentially peace of mind. You would

know where you would have a problem if there was some interruption of the business. And the third is that it enhances your operational efficiency. A lot of physicians don't really know exactly how their business operates. They entrust it to their office manager or their business office manager and this is a way to know exactly how your business is operating. You can perhaps find ways to operate more efficiently.

Frank:

That's a good idea. The other part of your plans, and we've talked a lot about technology, but the other part is actually more of administrative. As I mentioned earlier, you've got employees, you've got patients. What do you do in a case of some sort of disaster? So again, if it's a localized problem, computers go down, you lose power to the building, etc; those are fairly easy to come up with some backup plans.

Larger disasters: for example, if you're not too far away from a railroad track and they have a large chemical spill and they have to evacuate the area, you need to have some kind of plan in place of okay, what's the fall over. Is there a way to transfer the phones over remotely, is there a way, again, as I mentioned earlier, is there a way to contact patients? Is there a way to maybe switch to another office if you have a larger practice? So those are things that you have to think about. It's easy to focus only on technology, but the actual business. I mean, we did work for airlines. They don't really care that much if the computers go down because they can write the tickets by hand and they have procedures for that. So it's something that you have to think about.

Peter:

What exactly is a hot site?

Frank:

There's different ways of doing a backup. One is to have, for example, your main server have a computer that is an identical match and you are able to bring up the new machine fairly quickly either swapping out a hard drive or restoring the tape to it and you can bring your business back online.

A hot site can be where you actually keep a full set of computers at another location where you can take your tape backups and restore it and run from that location. So, that would require having connectivity to both offices and having a way to make sure that you can synchronize what you got.

So for example, if you're using Microsoft Outlook or Exchange server, you can actually set up two servers that constantly talk to

each other and they're actually backing each other up. So if one goes down the other one will still be working. So different variations and levels of that kind of what we call redundancy that allow you to recover a lot more quickly.

Peter: The typical medical practice would be in one location so it would probably be a good idea to either have a backup server or maybe their primary server that has hot swappable drives or something like that that can get them back in business within a matter of hours.

Frank: Yeah, one of the really least expensive ways to protect yourself is to set up what's called a RAID, as it sounds, R-A-I-D. A RAID system is just a method of using multiple hard drives to allow for failure of one. So, there's different levels of RAID. For example, RAID 1 is when you have two hard drives and the machine is writing to both hard drives. And so the way that they're set up, anyone of them can fail and if the machine happens to have what's called hot swappable [drives], in other words, you can pull a hard drive out when a machine is still running, you can quickly pull out the bad drive and stick in a new one and over a period of time the new one will heal itself against the other ones.

So that's going back to what you said earlier about man-made disasters. That's usually the one that hits the hardest, is hard drives go bad. The server is on for a long time. They do have a rating, so many hours' mean time between failures, so after several thousand hours, a hard drive can fail especially if it gets overheated or something. So having a RAID system is, again, it's relatively cheap nowadays if you order a computer from Dell or one of the big guys like that, you can have that put in for very little money.

That's the first level. The second level would be to have, well along those lines you can buy other parts of a computer that would make it redundant like two power supplies and two network cards and just anything you can have that if one fails the other one can pick up. So the next level would be to have a clone of that computer; a fully blown machine, everything's ready to go, and at this point here it would be one that could take your backup drives and within an hour or two you would have it restored and running.

So there's variations of that; depends on the operating systems and the software you end up buying.

Peter: We've kind of talked about the disaster recovery plan and we've also touched on continuity insurance. I guess another thing that

physicians may want to look into is overhead insurance. Continuity insurance tends to reimburse businesses for interruption in cash flow, but in some instances particularly if you're a physician who's buying into a group to become a new partner, you might want to consider something that may cover your overhead as your responsibility as partner. And they actually have types of insurance that can cover for that as well.

Frank:

Yeah, I think it's back to those kinds of cases of penny wise and pound foolish. Obviously everything costs money. It's a matter of really sitting down and doing an honest analysis of how much do I lose if I'm down for an hour, for four hours, for a day and then figure out the opportunity cost there. If you feel that you could shut down for a day and not be hurt too badly, is that cheaper than buying an insurance policy or the different levels of insurance?

In project management, there's risk management. Risk management is just a way of how do you deal with risk. In some cases you can mitigate risk, which says, what can I do to lessen the risk? I mean there's always the risk out there but I can do things to protect myself. For example, I can go in the car and put on a seatbelt so I'm mitigating the risk of being hurt. It's not one-hundred percent but I'm helping out. You can do avoidance which says I just shut down and not take the risk. And another one is called transfer, which means you're transferring the risk basically to an insurance company. They're assuming the risk and you're paying them for it.

So there's ways of sitting down and looking at. I think a lot of times people just look at the outright costs as opposed to what does it cost you if you don't. And you really have to look, going back to what you said a little while ago about looking at what does your business cost you, how does it run, all the cash flow, all those kinds of financial data that you have to really use and so okay, based on this, is it worth my buying a policy that costs X but I don't have to worry about any of this stuff?

Peter:

There's actually data out of FEMA that says that 40% of small businesses would not open after a disaster. I wonder how many practices in New Orleans closed and how many of those closed for good.

Frank:

Yep, and again, a lot of it goes back to even the simplest level of disaster recovery plans. Say you're a one man practice, you have one computer and what do you do? What if someone comes in and

steals the computer in the middle of the night? I mean, you have to think at that level and unfortunately a lot of people don't and it's just getting into a habit of what do you do. Now obviously, if you've got paper records, that's a whole other level and what happens if those paper records get wiped out? That's one benefit of going to electronic medical records, because at some point you'll have all that duplicated and again by doing a lot of these other things we've spoken about, you'd always have that information to get back and running.

Peter: That's very true. Okay, well it looks like we're just about out of time. Frank, if medical practices were interested in getting some more information or maybe consulting with you, how can they get in contact with you?

Frank: Best way is to go visit our website at www.eviton.com. We've done work for a lot of different types of businesses, airports, medical practices, and trying to put project management into some of these plans so that all the bases are covered.

Peter: Very good. Okay, thanks again. I really appreciate it.

Frank: All right, thank you.