Anne Genge - What do I do in case of data loss and how do I recover my data?

Dr. O'Keefe: You must have your head in the sand and if you're not hearing and reading every day in the media that cybersecurity is a huge issue in society, not just in healthcare or dentistry. I want to bring the Canadian dentists and dental team up to date with major issues in Cybersecurity, so I've invited a great friend of Oasis Anne Genge who's a certified privacy and security professional to come back and answer some questions for us. Anne Genge, thank you for coming back again to give us your advice. I know you've highlighted in lots of our short interviews that prevention is the key, but sometimes stuff happens, so what can I do if I do have a data loss, what can I do to ensure that it can recover from a data loss event?

Anne Genge: John, you know, we talk about backup almost every time we have discussions here on Oasis and the reason we have to keep bringing it up is I still see people looking to their backups at a time of disaster and those backups have either not been configured properly or there's been a corruption. These backups, no matter what form they take, must be tested. You have to do a fire drill to ensure that data is good. We also need to be taking an approach with backups that we have as many as we can afford to do, so that we've got lots of different medium to go to, depending on the type of disaster we have. If you have a backup drive just sitting next to your computer and it's backing up, that's fine, but if you have a fire or flood that's not helpful, so you need to have onsite and offsite.

Anne Genge: Offsite can happen on a backup drive or you can shoot it to the cloud, these will allow you a more predictable ability to recover. The best thing that we have now, about 18 months ago, virtualization became much more popular and affordable in the dental industry, and what this is, is it allows dentists to have a smaller computer sitting somewhere on the network that runs the same data to it as their existing server. What's beautiful about that is that it really delivers almost zero downtime if something should happen to the main server. It's also protected from ransomware. So, what that means is something bad happens to the server, really, literally a switch can be flipped, and people can keep on working, even keep taking x-rays in the face of that disaster while the other server is being fixed or replaced. That's really where we want to be.

Dr. O'Keefe: So, you just have to have a plan B parallel server ready to be switched on. Is that right?

Anne Genge: That is the best-case scenario. What's beautiful about it now is this is readily available, has been working in our industry now for, like I said, about 18 months and it's not that expensive. It's maybe $150 to $300 a month. But when you think about it, all it has to do is save one hour of downtime and it's already paid for itself. Additionally, it's backup that's protected from Ransomware.

Dr. O'Keefe: So, where would I go to to look for that type of service and, you know, check out the different options?

Anne Genge: My company does this routinely. We deploy these every week in dental practices across Canada. There are some IT providers that have the proper skill sets of know-how to deliver that. They may not get the same price point. But you know, there are a number of very good certified security professionals that do know how to deliver virtualized backup.

Dr. O'Keefe: So, virtualized backup is what I go knocking on the door and asking for?

Anne Genge: Absolutely, this is your get out of jail free card because it also allows you to everyday test to make sure that the data is valid.

Dr. O'Keefe: Anne Genge, thank you for this interview.

Anne Genge: Thank you John.