**Tailored Action Plan - Colette-20240827\_095828-Meeting Recording**

0:02  
So you can leave the camera off if you want.

0:04  
It's all the one to us.

0:05  
But yeah.

0:08  
So just to kick off, was there any actions you took after we did the workshop with you down in there was down in tree.

0:16  
We met you, was it?

0:18  
That's right.

0:18  
Yeah.

0:20  
No, I didn't.

0:22  
It's a kind of an ongoing one on the list.

0:24  
So no, we didn't.

0:26  
Yeah, that's grand altogether.

0:27  
So just wanted to check in about that.

0:30  
So I'll just share a presentation on screen here and we can show you the tailored action plan we came up with.

0:37  
OK, so can you see something there?

0:41  
Yes, I can.

0:47  
So we're giving you tailored action plan today.

0:50  
So just explain what that is at the moment.

0:54  
We're building a website that will have kind of a fully functional version of the risk assessment tool that you helped us develop there in in truly.

1:05  
So the website version, the idea is that the person will fill out the risk assessment tool very much like you did on the Microsoft Forms version of us.

1:15  
And then this tailored action plan will be generated automatically on the spot kind of based on whatever responses the person gave to the risk assessment to.

1:25  
And it's the whole idea is that we'd be given kind of personalized advice to your business and just to highlight the areas kind of that specifically your business should be looking at.

1:36  
So that's the idea behind this thing.

1:40  
And so just again, what we're giving you today, it's based on the answers you gave to that risk assessment to at the workshop then Limerick.

1:47  
So the top three actions that we identified that day were to use immutable or air gap storage for your backups.

1:58  
Second thing was to always use multi factor authentication.

2:02  
And the third thing was to test your backups regularly.

2:05  
And so I'll go through these in more detail and we'll just ask you for a little bit of feedback after I present these each of the actions to you as well, just to see if it makes sense to you and if they're relevant for your business.

2:17  
So the first one is to use a mutable or air gap storage for your backups.

2:23  
So if you can just read down through this and let me know when you're finished.

2:26  
And then we go through it with a few questions.

2:31  
Will this explain what a mutable means?

2:33  
Because I don't know or it well, that would that would be good feedback for us to get so I can explain it to you once you've gone through.

2:43  
All right.

2:44  
But yeah, OK, yeah.

3:07  
And so we've just gone through the questions here.

3:12  
And so just #1 how do you feel about this advice in general?

3:16  
How does it seem to you?

3:18  
Yeah, I'm not, because I don't know what immutable means.

3:24  
I don't follow it 100%, but yeah.

3:28  
And so, yeah, just just to let you know, so that an immutable backup is it's kind of write once and read many times backup.

3:36  
So it's basically kind of, you can have certain kind of file systems that allow your backup data to be copied over and once it's copied over, it can't be modified in any way.

3:49  
So that just makes it more secure against things like ransomware and and an air gap backup is kind of a similar functionality, but I suppose it's a little bit easier to explain.

3:59  
It'll be like if you took an external hard drive and major backups onto the external hard drive and then unplugged that from the computer and turned it off so that it's completely disconnected from any network or computer device.

4:12  
That's considered air gap then, as in there's no connection between it and anything else.

4:15  
So that again is very helpful to protect against rats somewhere for our situation.

4:24  
And so the critical data set would be obviously the patient information.

4:29  
So we work in an orthodontic surgery like dental kind of.

4:33  
So the way we do our backups is they go there, there the hard drive is plugged in in the morning and then that it actually backs up every hour because the critical data set is being updated every hour.

4:47  
And so then we take that away.

4:50  
But obviously we, we, we put it in the next day.

4:53  
So it's never really, you know, it's always plugged back in, say, I don't know, unless we took away one every.

5:00  
I suppose it'd be expensive to keep taking them away and not use them again, wouldn't it?

5:04  
Unless we did 1A year or something.

5:05  
At least you'd have some kind of, Yeah, well, like I see it in your case there.

5:12  
So like you when you do have data that's changing very frequently, that does mean that you do have to be taken to backups frequently.

5:18  
So it might be worth looking into for yourselves to see could you find an online backup solution that provided?

5:26  
So at the moment you're, you're using kind of, I suppose you could kind of air gapped in the evenings, but it's connected all day.

5:32  
So that means it would be susceptible to something like ransomware where if you had if you had a cloud backup service that gave you a mutable backup, that would that would be kind of something that would probably suit your business.

5:46  
Yes.

5:46  
Yeah, definitely.

5:47  
I should look into that.

5:48  
Yeah.

5:49  
OK, that's a good idea.

5:50  
Yeah.

5:52  
And so apart from that.

5:54  
So were the steps clear and helpful apart from just that immutable air gap thing?

5:59  
Yes, I definitely understand the logic behind it now.

6:01  
Yeah.

6:02  
Great.

6:03  
Great.

6:05  
And can you see any barriers that would prevent you following the steps?

6:10  
And I do just because there's people who provide the software over in the state, so they give you very specific instructions on how to do everything.

6:20  
So I'm not sure if they would allow us to connect to some sort of cloud based one, but they might provide the service themselves possibly, or I might just follow up with them and see if they could suggest anything.

6:35  
They don't really allow you to have to connect the server to any external company, like you can't have iTunes on it or anything like that, you know.

6:44  
So I should probably just to check with them who we could if it's something we could do.

6:51  
So is, is your set up like that you have kind of it's a patient patients records kind of software that runs on its own physical server in your office.

7:01  
Exactly.

7:02  
And nothing else is good on that server.

7:04  
Yeah, yeah.

7:07  
So it's yeah, it's definitely worth talking to your vendor there.

7:10  
And like, it might be like, I don't see any reason why you wouldn't be able to use an online backup service to just, you know, you'd be copying off the server to an online cloud storage thing.

7:23  
So that that could be something that would work.

7:25  
But like you said, it'll be your vendor, be the person that'll kind of be able to guide you the best there anyway.

7:31  
Absolutely.

7:32  
I'll have a chat with them.

7:33  
Yeah.

7:34  
And do you have any suggestions here how we could have improved that particular action?

7:39  
No.

7:39  
I suppose that you're always best to assume that anybody you're talking to is stupider than you.

7:45  
So maybe just, you know, have the, the terms explained before the, you know, because when you're reading that, if you don't understand the initial term, it, it wouldn't make that much sense, you know, So just like it's for dummies, you know, like I know you're, you're, yeah, perfect.

8:05  
No, that's that's, that's great.

8:07  
And so we go on to the second piece of advice here.

8:10  
And so this is always use multi factor authentication.

8:13  
So you can read down through that there and let me know when you're done.

8:17  
Sure.

8:17  
Yeah, Yep.

8:38  
OK.

8:39  
And so we go through the same questions again here.

8:42  
And so how do you feel about this advice?

8:45  
Yeah, I feel like it's, it's probably good advice.

8:49  
I think for every, you guys are probably going to be dealing with an awful lot of different businesses.

8:56  
So you know, it mightn't be applicable to every business.

9:00  
Like I'm trying to think of a way we could use it.

9:03  
We do use the multi factor thing for when we're taking credit card payments, for example.

9:08  
So you have to type in the CCV or whatever.

9:12  
But yeah, I don't know where else we could use it really.

9:20  
So yeah, I'm not sure.

9:22  
Like we send emails and stuff, we don't really use anything on that, but maybe that could be more secure.

9:30  
Possibly.

9:30  
So yeah, even just for the, I assume you've a few kind of desktop computers around the office that different people are using.

9:39  
Yes, we do, yeah.

9:41  
So they're kind of left on all the time because they'd be chair side and there'd be somebody after all the time.

9:47  
So they don't really log out and log in and stuff.

9:50  
We just turn it on in the morning really and off in the evening.

9:52  
That's it.

9:53  
Yeah.

9:53  
Yeah.

9:54  
So that that that'd be a bit of a a risk there.

9:57  
So that could be something you might look at and it's possible to use multi factor authentication for those logins.

10:05  
But anyway, yeah, just just something to think about and are this, would you say the steps are clear enough there and helpful?

10:13  
Yes, yeah.

10:15  
And then So what barriers would you see to following these steps?

10:20  
You kind of mentioned one there.

10:22  
I guess that it doesn't, it wouldn't really fit with your kind of current workflow if you've got the computers on all the time.

10:30  
Yeah, I suppose like potential barriers, it's just trying to identify maybe like I see suggestions there.

10:40  
I suppose it's hard to do it for every person's business, but it may be if there was a way you could help people identify the ways you could use MFA.

10:52  
You know, I, I don't know what you need to know more about their, their workflow and things like that.

10:57  
Maybe you might need to go a bit more in depth, but yeah, I suppose again, going back to us being dummies, we mightn't know all the technology that's out there.

11:06  
So maybe there is some way we could be using it, but we just don't know about it, you know, that that kind of away.

11:12  
So maybe a few suggestions or something.

11:14  
Yeah, I guess if we kind of had examples of where you'd be using it, that might be some help anywhere of maybe, you know, like when you say multi factor authentication, we all just think of our you know, when we're trying to do something on our phones and then we get the text or whatever.

11:31  
And so that's what we know about it.

11:34  
But maybe there is, maybe it's applicable in other situations, technology, you know, that we don't know about or maybe it isn't.

11:44  
Well, yeah, I guess so like most people would know it from banking.

11:47  
You know, there's nearly every, I suppose online banking thing always uses and you know, there's also some code you have to put in and but say, I'm just trying to think for your own business now, like would you use any accounting software that's in the cloud?

12:02  
Or do you know even like for your e-mail, would that be Gmail or, or what would you use for your office e-mail?

12:09  
We do have Gmail, yes, that's right.

12:11  
Actually our web designer was trying to get into it recently.

12:14  
So he had the we had the multi factor for that.

12:16  
All right.

12:16  
Because except it kept sending the the code to the.

12:20  
Yeah, Yeah.

12:21  
So we do have that.

12:22  
All right.

12:22  
Yeah, Yeah.

12:24  
Well, that's, that's an important one.

12:25  
Any sort of, it's good that you're using it there.

12:28  
But yeah, if there's, yeah, there could be other things like that.

12:31  
And like I said, even for the log on for your Windows machines, it'd be possible to set it up there if you wanted to follow that up.

12:39  
Cool.

12:39  
So we want to the last piece of advice there.

12:44  
And so this is to test your backups regularly.

12:46  
So you can just read down through that there.

12:49  
Yeah, yeah.

13:01  
Actually when I saw this, it reminded me that I actually did do something.

13:05  
After the workshop, I did contact the provider of the software and I asked them could we test the backups now.

13:14  
So the base, he said there's not a way of testing the backups because basically their backups means deleting the whole database.

13:23  
And it's like if someone deletes your database or keeps you ransomware or whatever, you can rebuild the whole database from this backup.

13:31  
So they said there's no way to actually test it.

13:33  
But they did tell me that what I should be doing at the end of every day is just checking the the hard drive itself and making sure that there was a completed backup for like on the hour every day and just check that.

13:50  
So we made it, we made a log book then just to check that there is an active completed backup at the end of the day just before we plug it out.

14:01  
And and we also came up with a system of reporting any problems with the drive itself.

14:07  
So it could be replaced easy.

14:08  
So we did do something actually.

14:10  
That's great.

14:11  
Yeah, yeah.

14:12  
And that, that's very worthwhile action you're taking there because that's, I suppose there's two parts to testing your backups.

14:19  
The kind of first part is checking that they've actually written.

14:23  
So that's what you're doing kind of by checking and that at the end of every day.

14:27  
And because like, a hard drive could fill up or whatever, you know what I mean?

14:30  
And you could think that the backups been taken and nothing's happened for weeks.

14:33  
So that's, that's great that you're doing that.

14:39  
Cool.

14:40  
So we go on to the questions there.

14:42  
Yeah.

14:43  
And so how do you feel about this advice?

14:46  
Yeah.

14:46  
Yeah.

14:47  
That's good advice.

14:47  
Yeah.

14:49  
And that seems all clear enough and helpful.

14:52  
Yeah, absolutely.

14:53  
Yeah, yeah.

14:53  
And I was able to follow the steps.

14:55  
Yeah, yeah.

14:56  
I don't see any potential barriers.

14:59  
Possibly they might need some, you know, somebody who was less, less tech savvy might need some specific instructions on how to test the backups, but I suppose depends on what kind of backups you have as well.

15:12  
So, well, I thought it was interesting there with your particular product that you're using that the vendor said that there wasn't an easy way of testing the backup.

15:21  
So it's, I suppose that is a bit of a barrier.

15:25  
Yeah, Yeah, that I suppose.

15:28  
Yeah.

15:28  
I, I thought it'd be, you know, there might be some way you could do it externally, but he said, no, it's basically deleting your database and starting again.

15:36  
So he said, you know, you can't just do it on a on a whim, but you just, it kind of makes you a little bit worried that you're just kind of tested and trusting them that it does work.

15:45  
But yeah, it'd be like I'd nearly you could press them a little bit about that because it should be possible for you to set up say like a test server.

15:54  
It could even be on the same machine that the software is currently running on.

15:59  
So that you'd kind of have your production one that's actually keeping your records.

16:03  
And then you could have test one that's just for testing backups, you know that you could, yeah, rebuild the database.

16:08  
And that would that might be something that they'd be able to help you with.

16:11  
But yeah, they kind of, they might need, they might need a little bit of a push.

16:15  
OK, perfect.

16:16  
I'll go back.

16:17  
They might have been just pulling me off with an easy answer.

16:19  
Maybe.

16:19  
Yeah, Yeah.

16:20  
You know, that can happen.

16:22  
Yeah.

16:22  
Absolutely.

16:24  
And so is there any other suggestions you could make and how we could improve that?

16:30  
No, I don't think so.

16:31  
I think that's so I suppose I remember at the workshop there was a little bit of information on the different types of backups.

16:39  
So I remember taking a few notes on things like that.

16:44  
So yeah, that was, that was good.

16:46  
I I thought, you know, to tell people the different types of backups that are that you could be using.

16:51  
OK, yeah, yeah.

16:53  
So just a little bit more of kind of, I suppose concrete kind of suggestions that we could include along with it.

16:59  
Yeah.

17:00  
So maybe examples that people wouldn't have thought of.

17:03  
You know, again, like not being tech savvy.

17:06  
We're we're OK in our place.

17:07  
We're told specifically what to do.

17:09  
Like you need to have two backups, you need to swap them out, you need to take one away from the practice, you know, things like that.

17:16  
So they give us step by step.

17:17  
But I suppose if you didn't have that guidance from your provider, it might be helpful to get it from you guys.

17:23  
Yeah, absolutely.

17:26  
And Grant, so that's us nearly done there.

17:29  
So just to sum up that these were the three actions we gave you and to use immutable air gap storage for your backups, to always use multi factor authentication and to test your backups regularly.

17:41  
So just First off, are there any other cyber risks that you're surprised didn't kind of come in in the top three?

17:47  
Is there anything you kind of know about your business that you would have kind of thought might end up there?

17:53  
Well, I was interested in the subject because we'd just done renovations and we had a kind of an idea that a network point, like a physical network point plugged into each computer is a little bit more secure than connecting them to the server via Wi-Fi.

18:16  
So we were kind of thinking about, you know, the best infrastructure wise and all that.

18:22  
So that's why I was kind of interested in the workshop.

18:24  
Now, I didn't really hear anything on that, so I wasn't sure.

18:28  
Maybe that wasn't, you know, I, I could have asked a specific question, but yeah, I would be interested in in knowing that.

18:37  
And also the other information I was kind of looking for was if there was anybody in Kerry who provided a service where they would come in and kind of audit the place and just say, look, you're not doing this right.

18:50  
You could be doing this better.

18:51  
This is a big risk here, you know, something like that.

18:56  
I'm not sure if you have any information on that.

18:59  
But if you were working, I, I presume you're trying to do the this yourself in the long term, would that be a service that you you are doing?

19:06  
Well, there's actually, I'm trying to, there's an organization called Cyber Ireland and they have a directory of cybersecurity consultants.

19:15  
So it's kind of something that we're hoping to look at down the line that we could kind of, I suppose, yeah, kind of have a list of cybersecurity consultants that specifically cater to SMEs and a lot of them will be kind of working with bigger companies.

19:31  
So it's just trying to find the people that kind of have the skills and the experience with SMEs.

19:36  
So that's something that we're looking at down the line, but we don't have it up and running yet, I'm afraid.

19:41  
Yeah, no, that's fine.

19:43  
So, yeah, just for somebody like us who was doing renovations, maybe things that, you know, you could do infrastructure wise, like, you know, I know they were, there's different types of cables and connections and things that would be more secure.

20:02  
Just kind of getting second hand information from other orthodontists who had done renovations and they were saying, oh, you should look for this type of cabling and stuff like that and.

20:14  
Yeah, that's kind of news to me as well, to be honest.

20:16  
So, yeah, yeah.

20:18  
And so they were basically saying to move away from wireless networking.

20:23  
And yeah, they were saying to have a network point, a physical network points plugged into the back of each workstation is, I don't know, they were saying it was more secure than having them all on Wi-Fi.

20:37  
I don't really know why, but I don't know, maybe it's maybe it's less open to hacking or something like that.

20:43  
So I don't know really.

20:44  
Yeah, it's it's, it's kind of a bit of a like it kind of makes sense in one way, as in, you know what, somebody definitely has to have physical access to your office to use the wired connections.

20:56  
Whereas if it's wireless, theoretically that they could break into it.

21:00  
But that said that if you if you're using kind of, you know, kind of a good quality wireless router with good encryption, I don't, you know, that's not really regarded as too much of A risk.

21:11  
Yeah.

21:13  
But yeah, Yeah.

21:17  
So I think that's us done for.

21:19  
We have just a quick survey, if you wouldn't mind filling it out.

21:21  
It'll take you kind of less than a minute.

21:23  
So if I pop that in the chat, Sure.

21:26  
Yeah.

21:26  
Would you be able to?

21:27  
Yeah.

21:27  
Brilliant.

21:29  
Just stop sharing there.

21:36  
So you should have a link there now if you click on that and then.

21:39  
Yeah.

21:47  
So this is all anonymous.

21:48  
So you can be as honest as you want here.

21:51  
Yeah, no problem.

22:16  
No, that's great.

22:19  
So and just before you go, we're kind of nearly ready with a version of that website that I mentioned with the kind of newer version of a risk assessment tool.

22:28  
So if you'd like, we can contact you when that's done.

22:30  
And you could have go off that.

22:32  
And there's there's different resources up there as well.

22:34  
And there'd be kind of e-learning modules on this and some other resources as well.

22:40  
So and if you're interested in that, we could give you a shout when that's up and running.

22:45  
Sure.

22:45  
Perfect.

22:45  
Yeah, that'd be great.

22:46  
Thank you.

22:47  
Brilliant.

22:48  
OK.

22:49  
Thanks, Emilian for taking the call today, Kales, and thanks for your time.

22:52  
Appreciate it.

22:53  
Take care.

22:54  
All right, Bye, bye.

22:56  
Bye.

22:56  
Bye.

22:56  
Bye.