**Risk Assessment Tool Pilot- Ciara-20240402\_150413-Meeting Recording**

0:02  
And this is just when you're filling out the form, just to maybe think your thoughts out loud, what you're thinking of the questions, if they're relevant to you or if they're not like because still in development at this point.

0:15  
So we just want to make it as relevant to SMEs as we can.

0:20  
So that's perfect.

0:21  
I'm good at thinking out loud.

0:23  
That's good, That's perfect.

0:25  
So, OK.

0:27  
Do I need to chair my screen or.

0:31  
No, it's OK if you want to go off your screen.

0:33  
I have it here on the as well.

0:36  
I'll follow along.

0:38  
OK.

0:38  
So I'll just start now.

0:40  
Yeah, perfect.

0:42  
OK.

0:42  
So question number one is do you consent about the information, have the opportunity to ask questions.

0:49  
So I'll just take all of these understand the right to refuse to participate.

0:53  
Understand that I give.

0:54  
Yeah.

0:55  
Understand my data.

0:56  
So the idea is you have to take all.

0:58  
Yeah, Yeah.

1:00  
So.

1:00  
Well, at first glance it looks like you'd only have to take one.

1:03  
So maybe take all that.

1:04  
Apply.

1:05  
Perfect.

1:07  
Yeah.

1:08  
I consent voluntarily to be a participant.

1:10  
Yes.

1:11  
So next, are you a sole trader?

1:14  
No.

1:16  
How many employees are in your business including all part time and full time staff?

1:22  
So we currently have eight what sector 2222 prison, hospitality, transport, retail would be.

1:35  
We're software so I guess it would come in under information media and telecommunications.

1:42  
I guess I always struggle with these drop downs you know that with when those are kind of standard and I'm like we don't really it's hard to know OK who manages the cyber security dedicated team outsource team, shared one employee myself.

2:02  
No one other.

2:13  
I mean, like, it's I suppose if you think of like cybersecurity in terms of like people being responsible for like their own emails, not clicking on links or things like that, I would say it's shared.

2:26  
But then if you look at like cybersecurity in terms of like putting in firewalls and stuff in our server, yeah, I suppose that's what we're more looking at, like the protect.

2:38  
But I suppose that is something that we could actually specify in it what we're looking for.

2:43  
Would you have a dedicated cybersecurity team like, for those things?

2:47  
No.

2:49  
Like it's it's kind of, it's a little different Elements are taken care of by different people.

2:54  
You know what I mean?

2:55  
Yeah, the overall responsibility probably falls on me.

2:59  
But like, yeah, I would probably say it's shared maybe.

3:06  
Yeah, that could work.

3:07  
Yeah.

3:07  
I'll actually make a note of that to specify it, what we're looking for, yeah, because that's, you know, that's kind of a broad term.

3:16  
It can be interpreted a lot of different ways.

3:18  
Yeah, that's true.

3:20  
That's OK.

3:23  
Do you have cyber insurance?

3:25  
That's easy.

3:26  
Yes, No, no.

3:27  
Can customers make purchases on your website?

3:34  
I have a website where customers cannot make purchases on it.

3:41  
How is your business website managed or maintained?

3:48  
Outsource third party website?

3:50  
Set up a third party, not regularly maintained.

3:53  
I managed and maintained.

3:56  
Do you feel confident managing the cyber security?

4:04  
Not me, no.

4:06  
So like on question nine there, you know outsourced third party.

4:11  
I manage it.

4:11  
Or I'm not sure there could be another option there of like someone on my team.

4:17  
Yes, perfect.

4:18  
The right answer here for me is I manage, but it's not I as in me personally, like you're confident it's someone I as in it's internal.

4:26  
Yeah, perfect.

4:27  
I'll make note of that.

4:28  
Yeah.

4:30  
And do you feel confident managing the cyber security?

4:34  
So again, so this is where, like me personally, I don't feel confident, but I know it is being done by somebody who is confident, You know, Yeah, probably say yes for that.

4:47  
Do you have an inventory of all your digital hardware list of all computers, mobile phones?

4:51  
Yes, we do.

4:54  
Well, somewhat, I think is probably the best answer.

4:57  
It may not be up to date.

5:00  
Yeah, it's on some Excel spreadsheet tracker somewhere.

5:03  
I don't know, it's fair.

5:05  
Silver.

5:06  
Yeah.

5:08  
Do you have an inventory of all the software used for your business?

5:12  
Same we have a list actually.

5:14  
That is the project for my head of operations at the moment, updating both of those Packers.

5:21  
That's good.

5:22  
You're on top of that.

5:23  
So, well, yeah.

5:25  
Do you or members of staff use their own personal devices?

5:29  
Yeah, we do.

5:31  
Do you have antivirus?

5:36  
Yes, on some, because it would be on our computers.

5:38  
But like people's personal phones?

5:40  
No.

5:40  
And they do access their emails from their phones.

5:43  
OK, Yeah.

5:44  
So yeah.

5:46  
Do you have spam filters enabled on your work e-mail?

5:49  
Yes.

5:51  
On it.

5:51  
By e-mail provider.

5:52  
Yeah.

5:52  
We use Gmail, so it takes care of all of that.

5:56  
Our work device is wiped off all data when they're no longer being used for the business.

6:02  
Yes.

6:04  
Yeah.

6:05  
When we get, like, we give people a laptop and then they leave the company, they give it back and then you wipe it.

6:10  
Yeah.

6:11  
OK, Yeah, that's perfect.

6:12  
Where we would then recycle it and give it to another person, you know?

6:15  
Yeah.

6:15  
Yeah.

6:16  
How do you keep the software on your devices up to date?

6:21  
Manual, automatic guess.

6:29  
Manual.

6:30  
Like, you know, your iPhone.

6:31  
It's like it's time to update.

6:32  
You have to manually do that, certainly on phones.

6:35  
Yeah.

6:36  
It's manual.

6:38  
Yeah.

6:41  
What type of data does your business collect?

6:45  
Personal.

6:48  
No, no sensitive design documents.

6:54  
Yeah, intellectually back to you because we have the, the hotels and venues that we work with.

6:58  
We have their images, we have their brochures, their price lists, etcetera.

7:02  
So that would be intellectual property.

7:04  
Yeah.

7:05  
Yeah.

7:08  
Are you aware of your obligations on the GDPR to report a personal delivery?

7:12  
Yes, I did know that.

7:13  
Where do you store cloud storage?

7:20  
Yeah, everything is in the cloud.

7:23  
So yeah, Do you encrypt the data you store?

7:27  
Yes, we actually do.

7:28  
It was a new thing we brought in only about a year ago.

7:32  
That's very good.

7:33  
So do you process customer payments over the phone?

7:46  
We can, but we really don't.

7:49  
It probably happens once a year, if that.

7:53  
So I'm going to say no.

7:54  
Yeah, that's fine.

7:55  
OK.

7:56  
Do you share customer data with any third parties?

8:18  
How do you handle data backups For critical data?

8:23  
Yeah, we do have backups.

8:27  
I would say that they are made idea.

8:30  
How often do you compute a data backup?

8:36  
I would have to ask Chris.

8:38  
I'm not sure it is regularly.

8:46  
Yeah, that'd be fine to say.

8:47  
I'm not sure on it if you're.

8:48  
Yeah, just say I'm not sure.

8:49  
I think I'm actually going to ask.

8:51  
No, just I have my own interest.

8:55  
Write that down.

8:57  
Do you have an immutable or air gapped backups.

9:01  
Oh Jesus, I don't know what that means.

9:03  
Oh, here we go.

9:08  
Air gapped means having no direct connection to the Internet.

9:18  
I don't think so.

9:19  
That would be like if it was on a hard drive or something.

9:22  
So it's not actually on the Internet anywhere.

9:26  
It'll be on a hard drive being like exactly then then no we don't.

9:31  
No, everything we have is in the Are your backup the data backups tested?

9:43  
I'm not sure I'm going to write that down, Jim, do you follow Role based access control?

9:58  
This is where employees only have access to information software that is needed for them to complete their job role.

10:09  
I would say somewhat, yeah, because we stick, we store things on the G on it like a central G drive.

10:16  
So there's definitely people have access to stuff that they don't need.

10:22  
Yeah, yeah, yeah, that that is true.

10:28  
Who has admin privileges?

10:32  
Myself, another employee and outsource third party.

10:43  
We do work with an IT company and they would have some configuration settings for our our servers.

10:52  
Yeah.

10:54  
Do you have multi factor authentification?

10:58  
Yes, we do.

11:00  
For some I would say not for everything.

11:12  
This is critical.

11:15  
I'll just say for some what type of MFA, well it depends on the thing, right?

11:23  
So like for the bank, we've got an app.

11:26  
Yeah.

11:27  
So you can take sometimes it's called SMS, Yeah.

11:33  
Yeah.

11:34  
Hardware token.

11:35  
That's like for revenue, isn't it Like for uploading to Ross, you've got like a token that's on your device.

11:42  
Yeah.

11:44  
Yeah.

11:44  
So we have all of them.

11:46  
Do you or any of your employees share passwords with one of their job?

11:51  
Yes.

11:54  
Like for our Instagram or whatever, we would.

11:57  
Yeah, Yeah.

11:59  
Do you require staff passwords to have a minimum length?

12:04  
Like so?

12:05  
No.

12:06  
Do you or staff use password managers?

12:09  
Some do, but not everybody.

12:12  
OK do you enforce block listing passwords?

12:16  
This is where certain passwords are not allowed to say they're too easy to guess.

12:19  
No, don't do that.

12:22  
How often do you and your employees engage with cyber security training, ad hoc, no formal training?

12:31  
Yeah, we did.

12:33  
There was a company that was near off, you know, in the same business park as us a few years ago.

12:39  
And they were doing, this was around the time of GDPR and they had like an e-learning portal where we could log on and watch videos and answer questions and get like a certificate.

12:50  
And so I got everybody to do that at the time.

12:54  
But I don't know what happened to that company.

12:55  
Did they go out of business?

12:57  
I don't know.

12:57  
And we didn't keep up with it.

12:59  
OK.

12:59  
It sounds, yeah, that sounds good though, that you're able to get certificates and everything with us.

13:06  
Yeah, that was literally back in, I'd say 2018-2019, like way before COVID.

13:12  
And most out of all the staff that I trained in that, there's only one guy that's OK, two people that still work for me.

13:19  
So our team has changed, you know.

13:22  
So yeah, the true answer is, yeah, there's no formal training.

13:26  
Yeah, that's fine.

13:26  
Yeah.

13:28  
What methods have you or your staff undertaken?

13:32  
Videos.

13:33  
Yeah.

13:34  
Courses, I suppose is probably And then e-mail announcements like, you know, don't click this thing or there's a phishing scam.

13:43  
You know, we would have alerted people to that, Yeah.

13:46  
And our employees were required to report any suspicious activity.

13:54  
I would say somewhat, yeah.

13:55  
It's not consistently enforced.

13:57  
Like we, you know, we're a very faulty there's only eight of us.

14:00  
So it's like, yeah, you'd probably you'd probably say it anyway.

14:05  
Yeah.

14:06  
Yeah.

14:06  
Somebody's like, oh, I think I've been hacked or you know there was something.

14:10  
Yeah.

14:10  
We would say it like would you and your staff know what to do if a cyber incident occurs?

14:20  
No.

14:21  
Yeah.

14:21  
Honest answer is no.

14:23  
Do you have a business continue to plan in place.

14:27  
No.

14:28  
Jesus.

14:31  
Next.

14:32  
Follow the link if you resort trader.

14:34  
OK.

14:34  
I'm not go next.

14:37  
Thank you for completing Wow.

14:39  
The language used was understandable.

14:42  
Yeah, well, except there was some confusing things, but then you explained them, so that was fine.

14:50  
Well, I'll write that down here.

15:02  
And explained OK.

15:07  
The tool is easy to use, yes, please comment.

15:26  
Very relevant to my business.

15:28  
And yes, we're required for estimates to include the risks next thing.

16:02  
So all the feedback is the next thing SM ES will want is, I suppose maybe a report is that, is that what would come out of this like a risk of assessment?

16:13  
Yeah, yeah.

16:16  
And then with recommendations or steps to follow and potentially I think they'd want like, OK, your your risk is red.

16:29  
You know it's red.

16:30  
Your risk is very high.

16:31  
These are the things you need to do.

16:32  
But then these are people who can help you to do those things.

16:36  
OK, people.

16:37  
Yeah, people.

16:37  
Because what we're planning on doing is to that.

16:41  
The end goal for it is that it would be automatic tailored advice.

16:45  
So depending on your answers and it's tailored to you specifically.

16:49  
So then what are what we're thinking at the moment is the steps people can do to help them, whether they have no budget at all to give towards us, whether they have you know a low budget, a high a high budget.

17:03  
So doing that way.

17:04  
But that would be handy as well to add in people that could that could help them.

17:10  
Yeah.

17:11  
Because I think a big thing like for me is, you know, I wouldn't even know where to start, right.

17:16  
So definitely I already know by the answers that are given that there is some, you know, holes there for in my business, there's definitely some areas that we could improve on.

17:26  
And if I got a report saying, you know, your risk is medium yellow, these are the suggested actions, it's like, OK, that's great.

17:34  
That's a report.

17:35  
We don't have the expertise internally to do that.

17:37  
And so it's like, well, where's our next point of call if you could signpost us to, yeah, these are other, these are companies or consultants in Cork that can help with these areas that would be really helpful.

17:51  
Yeah, yeah.

17:53  
I'll make oops next thing hasn't even worked.

18:09  
Fiber because yeah, I would think that that's the biggest challenge.

18:17  
It's it's like we're all ostriches.

18:19  
Like our heads are in the sand.

18:20  
It's like La La La La la I don't want to know until it happens to us kind of thing.

18:25  
Most people want to be compliant.

18:27  
Most people want to be secure.

18:29  
And if they're told that there's a really grave error, most people could find somebody just to do something or, you know, but it's it's not, it's it's not like for me, it's just pure ignorance.

18:43  
But like, well, where would we go for help.

18:45  
I'm not going to the Yellow Pages looked upside the security cork like, you know, it's you want that recommendation, that referral, which I know is obviously very challenging, but it probably would be the next thing that people would ask, OK, I've got a report.

19:00  
What now.

19:01  
Yeah.

19:01  
Because we, we do want it to be just like immediately available and like action points that like that you can follow just yourself.

19:11  
Like if if it was that there was no budget, there's like, OK, well, here's how to set this up and this is free.

19:16  
You can do this yourself.

19:18  
And this will help with this kind of, you know, just to have that everyone is catered for whether they have absolutely no budget to put towards it or if they have loads that everyone will get something from the activity.

19:31  
Yeah, no, that makes sense.

19:33  
I mean, just even going through this, like if something's there that, you know, like the, the, the database or whatever of all of the the devices that are in your company, like that's a little bit of an inventory.

19:46  
That's a small project, a task that would have to be done internally.

19:49  
You're not probably getting a, an external company or a consultant to help you with that.

19:53  
Like if it's an SME, it'll probably be the head of HR, the head of operations or the managing director or something that will do that.

20:01  
All right, everybody, tell me what devices you have.

20:03  
Who's got a monitor?

20:04  
Who's got a mouse?

20:05  
Who's got a laptop?

20:06  
Whatever.

20:08  
Or then doing the audit of you know the software platforms etcetera that's you know easy free things that people can do.

20:16  
It doesn't require any technical expertise.

20:19  
But then, you know, there's some other things that you mentioned there about like data backups and stuff that's like, OK, well, that's above my pay grade.

20:26  
I don't know how to do that.

20:27  
But I can ask somebody and, you know, so it's kind of breaking it out.

20:31  
This was of this is the non-technical to.

20:35  
Yeah.

20:35  
Done versus.

20:36  
OK.

20:36  
There's some technical things that need to be done that you may or may not need to get outside assistance with.

20:42  
Yeah.

20:42  
Because what we're thinking now is that we're actually going to see if we can set up a website where as you were saying earlier that there was a cybersecurity team where they gave certificates like with online training.

20:55  
That's what we're actually going to aim to do.

20:57  
So have the risk assessment tool there and it feeds back what their main areas that they need to do are.

21:04  
And then they can do the training with us and it's free and you get a badge with it.

21:10  
So you know it's recognized.

21:12  
Now this is all very early days and our hopes, so we'll see.

21:17  
But just that would be really good because like a lot of companies as well want to do the cyber security training for their staff from a compliance point of view.

21:26  
So if they were to have an audit, they'd be able to say, well, all my staff have completed this training within the last six months and here's the certifications to prove it.

21:35  
Yeah.

21:36  
So it would be benefit.

21:37  
It would be beneficial, definitely.

21:39  
Yeah.

21:40  
Right.

21:40  
Yeah, for sure.

21:42  
You could even charge for that like, you know, well, we're trying.

21:45  
We're trying to keep it free.

21:46  
I think we do have the budget for us to keep it free.

21:50  
But OK, hopefully it's hopefully it plays out amazing.

21:56  
OK, Fab.

21:58  
Is that it or do you need anything else?

22:00  
Yeah.

22:00  
Is that.

22:00  
Did you submit some?

22:02  
I did.

22:03  
I hit submit There.

22:04  
Perfect.

22:05  
That's brilliant.

22:06  
I'll just stop recording there.