**Call with SME 3B 05/04/24**

Researcher’s voice in **bold**

0:04  
**All right.**

**0:04  
So we're recording there now.**

0:06  
OK, That's fine.

0:10  
**So did that link come through to your e-mail?**

0:12  
It did.

0:13  
I have it open now.

0:15  
**That's great.**

0:15  
**So the the first thing you see there is the kind of consent.**

**0:18  
So I don't know.**

**0:19  
Did you get a chance to read over the.**

0:21  
I'm sorry, I didn't.

0:22  
No.

0:22  
**Yeah, just that you can click on it there, It will open up.**

**0:25  
And just have a quick read of it continue.**

0:55  
OK.

0:56  
I'm a fast reader, so I'll go, that's great.

0:59  
**So and then as you're checking the the consent back on the other screen, if you can read out each one as you're as you're checking it, just read out the the accompanying text.**

1:20  
OK.

1:20  
I have read the information sheets entitled Information for participants, Risk assessment tools for SMEs provided on this research study.

1:29  
So I'm going to tick yes.

1:32  
I've had the opportunity to ask questions and as such understand the purpose and nature of the research study.

1:39  
I understand that I have the right to refuse to participate, refuse to answer any questions, and withdraw up to the point of data analysis without any consequence.

1:51  
I understand that the answers I give will be collected by the research team and used in their study.

1:58  
I understand my data will be used in the development of the risk assessment tool.

2:02  
It is planned to publish the findings in an academic journal.

2:07  
OK.

2:08  
I consent voluntarily to be a participant.

2:11  
**Yes, that's great.**

2:14  
Thanks very much.

2:15  
Will I continue on?

2:17  
Yeah, I'm a sole trader, Yes.

2:21  
**Oh, just to say what you're doing it already.**

**2:23  
But just to as you're going through, just read out each question as you come to it.**

**2:26  
And if there's anything that's confusing or anything, just say.**

2:29  
I know that.

2:30  
Say it loud enough.

2:31  
I know.

2:32  
**I I heard You're right.**

**2:33  
But just as you're going just to make sure you do it all the way down.**

2:36  
OK.

2:37  
Are you a sole trader?

2:38  
So I take yes, please follow the link.

2:40  
So it's a different form.

2:43  
Is that right?

2:44  
**Yeah, OK.**

2:48  
What sector?

2:53  
Probably education and training.

2:55  
There isn't one.

2:56  
Yeah, no, that's that's perfect.

2:58  
Who manage?

2:59  
No one.

3:01  
Who manages the cybersecurity?

3:05  
I suppose I do.

3:07  
To whatever degree will I put myself, I'd have awareness if there.

3:14  
**If there's no one else, I guess it's you by default.**

3:17  
Yeah.

3:17  
OK.

3:18  
Do you have cyber insurance?

3:20  
I don't.

3:21  
It was extremely expensive.

3:27  
Can customers make purchases?

3:32  
Not at the moment.

3:34  
So I'll I'll say have a website, but customers cannot make purchases.

3:40  
How is your business website managed or maintained and outsource professional managers?

3:53  
Oops.

3:57  
Do you have an inventory of all your digital hardware used?

4:09  
That means, like, I know what I have, but I don't have them listed out.

4:16  
So this means kind of a written inventory, I presume.

4:20  
**Yeah, that's right.**

4:21  
**Maybe that's something we should make a little clearer.**

**4:22  
But yeah, written.**

4:26  
Yeah.

4:28  
OK.

4:29  
**So say no.**

4:31  
Do you use your own personal device?

4:37  
Yes.

4:41  
Do you have antivirus?

4:42  
Yes.

4:45  
On all devices, do you have spam filters enabled?

4:56  
Can you elaborate on that?

4:58  
**Do you have spam filters enabled?**

**5:01  
And so I suppose if you're if you're kind of a sole trader, you're probably using something like Gmail or something like that.**

5:09  
I have a Black Knight OK e-mail and it's probably something they set up on it that you don't have to worry about.

5:17  
**I guess that it kind of Do you ever get like an e-mail into your inbox that it has a warning on it that says, you know this, they've gone into spam.**

5:25  
So I guess I do have a filter if they end up there, yeah, or work divided work devices wiped of all data when they're no longer being used for the business.

5:43  
Have not needed to do this yet, although can I ask something with this?

5:51  
I'm going to be giving an old laptop to my sister-in-law so I should wipe it.

5:58  
Is that right?

6:00  
**Yeah, it should.**

**6:01  
It should be wiped and kind of do a fresh install and would be the best thing to do in that situation.**

**6:08  
Just because once it's out of your hands, you don't really know kind of what's going to happen next.**

6:12  
But she's going to be doing things for me work wise, but it's more documents that I could upload then afterwards.

6:19  
**Yeah, like to be sure, because maybe were you using that laptop kind of for everything, basically for the business and there could be all sorts on there.**

6:27  
So yeah, yeah, OK.

6:33  
How do you keep software automatic and some I've automatic updates activated on all software applications and devices.

7:01  
Just today the Mac my PC has come up with and then I have Microsoft then there's Windows that I've or whatever it's called Office.

7:18  
I have an annual subscription to that.

7:20  
So yes, I get.

7:22  
I have automatic updates, but I have a choice whether I do it then or not.

7:27  
Yeah, yeah.

7:28  
OK.

7:31  
What type of data does your business collect?

7:34  
Personal data.

7:49  
So I'm just putting, I collect personal data, intellectual property data.

7:55  
Would that be my own stuff?

7:58  
**Yeah.**

**7:58  
It would include your own stuff.**

8:00  
Yeah.

8:04  
If I download something is that, does that fit with that too?

8:09  
**Well, like if it's something publicly accessible, do you mean or no that that that wouldn't really count I guess if it's publicly accessible.**

8:16  
**But if you, if you if you've got like your own training content, do you know that that's I suppose a business secret.**

8:22  
So that that would definitely count very much a secret.

8:24  
Right.

8:24  
And don't tell anybody.

8:27  
OK, 14.

8:29  
Are you aware of your.

8:30  
Yes, yes.

8:35  
Where do you store this data?

8:42  
OK, for this one I have a platform CRM I guess it is, I don't know called Coach's council which has all the security in built so I don't keep a lot myself.

9:04  
Yeah, but I do use cloud iCloud, so I suppose I'll tick that.

9:11  
And for other how would I describe it CRM or it's also LMA learning management system maybe that's more OK.

9:25  
**So it it are you saying it's both like so like customer relationship management and a learning management system kind of in one and it's, it's cloud based.**

9:35  
**Yeah, Yeah, I'd see, yeah, I'd, I'd just put that in that it's a cloud based CRM system that's like presumably only you have access to or.**

9:49  
Yeah, yeah, yeah, yeah.

9:51  
OK.

9:51  
I don't know that tipped.

9:56  
Do you encrypt the data that you store, do you keep the day?

10:07  
I don't.

10:08  
But do you think that system that I use does?

10:13  
**Probably not, unless you explicitly do it.**

10:17  
Yeah, sure.

10:19  
Yeah.

10:22  
Do you process customer payments over the phone?

10:24  
No.

10:27  
Do you share customer data?

10:28  
No.

10:29  
No.

10:32  
No.

10:33  
How do you handle data?

10:35  
Backups for critical data?

10:38  
Backups for critical data.

10:50  
I don't do the backups but they do so would I put I have automated backup scheduled.

10:57  
**So when you say that they do the backups is this your like your CRM.**

11:01  
Yeah stuff is it.

11:03  
Yeah.

11:05  
No.

11:05  
**I I I'd I'd say no in that case because yeah you wouldn't be quite sure what they're doing with it.**

11:12  
So I'll put I don't have a formal, Yeah, that you don't yourself have it like, OK, how often do you complete a data backup?

11:22  
iCloud.

11:23  
That's a constant.

11:26  
I don't know how often things are uploaded to the cloud.

11:33  
I don't do that.

11:34  
I should.

11:35  
I should do that?

11:35  
**Probably.**

11:36  
Should I?

11:37  
**Yeah.**

**11:41  
You're not alone in not doing it though.**

11:43  
No, I'll put ad hoc then.

11:54  
Do you give me advice at the end of this or when the results are compiled or.

11:59  
**And no, like we kind of don't have that built into this phase.**

12:03  
**But like we can keep you updated as we develop it and we'll be when this is finished, we'll be offering this as a free tool online.**

12:11  
**So at that point you'll be welcome to come and do it when it's further developed and then you'll get the advice.**

12:16  
**That's the kind of the next part we're working on.**

12:19  
OK.

12:19  
I don't even know what this means.

12:21  
Do you have an immutable or air gaps, backups for your business.

12:25  
Air gap means immutable means read only, air gapped means having no direct connection to the Internet.

12:37  
I don't really fully understand what that means, so I suppose the answer would be kind of no in that case.

12:44  
**Anyway they're they're they're kind of technical and they're like the ideal sort of backup would be where it's immutable because once it's written say to a hard drive or a cloud cloud storage backup that nobody can change it anymore**.

13:00  
**So even if a virus got onto it it wouldn't have the ability to write it.**

13:03  
**So that's a very secure form of backup and then air gap just means that it wouldn't be connected to your system or any computer network so that it's invulnerable.**

13:12  
Then in that case as well to being meddled with now the malware I have protection that wouldn't that's different to the that question is it.

13:21  
**Yeah it is.**

13:22  
Yeah.

13:22  
Yeah.

13:22  
**It's kind of I suppose it's it would the kind of cyber security it's always kind of belts and braces.**

13:28  
**You know what I mean?**

**13:28  
That one system can fail.**

**13:30  
So then you have to have an, you know another thing behind it.**

13:32  
**So kind of malware would be one step and then the immutable backup would be a further step.**

13:37  
Then again, OK, I'm going to take a screenshot of that.

13:53  
**OK**.

13:54  
Is your your data backup tested?

14:04  
I'm not sure.

14:14  
Can I will I give a copy of these because I can.

14:17  
There's a few questions there that I'd like to ask from the platform people that I, you know, the Ms.

14:25  
**and yeah, that that that should be possible.**

14:28  
**I'll have to double check with the the lead researcher, but I don't, I don't think there'll be any problem with that.**

14:33  
It's kind of not a bad idea, these kind of questions that maybe yes is the answer, but I don't.

14:39  
Yeah, I don't know.

14:41  
**Yeah.**

14:41  
Do you have admin privileges?

14:43  
Yeah, yeah.

14:48  
Do you have multi factor authentication again, if I knew what that meant, yeah.

14:57  
**So that that's like you know if you're if you get if you're accessing your bank's website that it'll often text the code to your phone and then you have to re enter that as well as well as doing your username and password.**

**15:09  
So it's kind of, you know, a second way of authenticating you or Gmail would often do it as well.**

15:15  
Yeah.

15:16  
Yeah.

15:20  
My system would have the double, you know, it's more GDPR compliant.

15:24  
Add the double opt in.

15:27  
**Oh yeah, Yeah.**

15:28  
And they have to have a password to.

15:36  
But I think that's different to what this is asking.

15:39  
**Yeah.**

**15:39  
No, that'd be different.**

15:40  
All right.

15:41  
OK.

15:41  
So no then would be the.

15:46  
But if I do have it for banking, do I put.

15:48  
Yes for some business critical?

15:52  
Yeah.

15:53  
**If it's for like it's for your business bank account.**

15:56  
**I guess that would count.**

15:58  
Yeah.

15:58  
It's kind of stretching it probably.

16:00  
**Yeah, a little bit.**

16:02  
OK.

16:02  
But it makes me look a little better.

16:06  
All right.

16:06  
Oh boy.

16:07  
Oh boy.

16:08  
What type of MFA do you have?

16:10  
Tickle that apply I think I should probably say no for the other.

16:14  
**OK.**

16:15  
Everybody who has a bank account and uses online has that.

16:19  
So that wouldn't really fit with what you're doing, I think.

16:23  
Yeah.

16:24  
**It's more kind of directly related to your business.**

16:28  
Do your passwords have a minimum length?

16:30  
Yes.

16:31  
The software enforces this.

16:33  
Do you use password managers?

16:46  
Me.

16:46  
I do, yes, for some of my passwords.

16:56  
Do you enforce block listing passwords?

16:59  
This is where, yeah, I'm not sure now because I if my client forgets their password then they go through the process of setting it up again.

17:09  
So maybe that's that's something I need to I can find out.

17:14  
How often do you engage with cyber?

17:18  
I'd have to say never would.

17:21  
You know what to do if a cyber incident occurs.

17:27  
Yeah.

17:27  
You guys know this from what you've been through too nice.

17:35  
I like to think I'm small.

17:40  
Do you know small for whatever that it wouldn't be but you?

17:42  
I guess you never know.

17:44  
Do you have a business continuity plan?

17:46  
Document how to prevent and recover from question six.

18:02  
It says I didn't answer, got to go back.

18:06  
Do you have an inventory?

18:18  
No.

18:18  
I thought I said no, I don't.

18:34  
OK, feedback then language use, understandable.

18:39  
No jargon used.

18:42  
Mostly I'd say.

18:45  
**So remember, hey, can you remember any bits that's that tripped you up and remembered that the immutable backup was probably one anyway.**

18:51  
But again if there's if I wasn't doing this on my own.

18:55  
So in a way that wasn't a problem because I could ask you and you explained it.

19:01  
**Yeah, I suppose we're thinking of the case when you would be on your own though.**

19:04  
**So I mean, it was kind of explained a bit, but it is still, that's a very jargon heavy question, that one.**

19:10  
**So we're kind of keeping an eye on it.**

19:13  
Yeah.

19:16  
So, comment on MFA, comment on the languages.

19:45  
So I wrote MFA and a couple of others were not clear to me, but were explained.

19:50  
The tool is easy to use, yeah.

20:05  
Relevant to my business, yeah, more than I probably realise.

20:19  
Beneficial exercise, then they go with comments.

20:26  
It's kind of the same, OK, I wrote.

20:28  
Highlights the gaps for me.

20:30  
For the relevance, I'm going to refer to that #36.

20:58  
I said Do you have any other feedback?

20:59  
Look forward to seeing the results on the app when it's finished, Grace.

21:04  
OK.

21:06  
Yeah.

21:06  
That's brilliant.

21:07  
That.

21:07  
**That's everything, really.**

**22:18  
And so have you any, like just general thoughts about the, the risk assessment thing there?**

22:23  
Well, no, I I guess what I wrote at the end there, it really does highlight that it's something you take for granted until there could be a problem.

22:38  
Yeah, Yeah, that's it.

22:40  
The insurance though is I looked into it for work I was doing.

22:47  
They eventually took it off the table because it's prohibitive, you know, it's hundredths.

22:54  
Yeah.

23:00  
Yeah.

23:00  
**And it's kind of taken off at the moment like.**

**23:04  
But yeah, it's, it's an odd one because yeah, it must be a tough one for the, the cyber insurance companies to figure on.**

**23:11  
As in, you know, it's a bit of a, how long is a piece of string when things go wrong.**

23:15  
Yeah.

23:16  
And so I'd say it's, it's kind of a new area.

23:18  
All right.

23:19  
Yeah.

23:19  
And we were found wanting, weren't we, with HSE?

23:23  
And then I don't know about yourself so much, but yeah, but it was a massive cost here, like.

23:29  
And you know, there's still stuff being sorted out over it.

23:32  
So I mean, yeah, after COVID, were you studying during COVID too, or did you come in after that?

23:40  
It's after that.

23:41  
But I would have been, yeah, I would have been kind of working online a bit during COVID, but that's basically, yeah, it's, it kind of exploded.

23:46  
Everything went online, but it went online very quickly and without service.

23:50  
Yeah.

23:51  
Yeah.

23:51  
Good.

23:52  
OK, Brian, that's fantastic.

23:55  
Good, good.

23:56  
If there's anything you can come back, great, brilliant.